ASTREA ACADEMY
SHEFFIELD
SAPIENTIA DUCET AD ASTRA

Social Media & Online Safety

POLICY

POLICY LEAD	Lorraine Yates, Trust Assistant Principal
REVIEWED BY	Sarah Naylor, Assistant Principal
APPROVED BY	David Boyd, Principal
DATE OF APPROVAL	September 2023
LAST REVIEWED ON	September 2023
NEXT REVIEW DUE BY	July 2024

Introduction and Aims

This policy aims to:

Set out expectations for all Astrea Academy Sheffield (AAS) community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)

Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the Academy gates and regardless of device or platform.

Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare Scholars for the risks and opportunities of todays and tomorrow's digital world, to survive and thrive online.

Help staff working with scholars to understand their roles and responsibilities to work safely and responsibly with technology and the online world:

- for the protection and benefit of the scholars in their care, and
- for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
- for the benefit of AAS, supporting the ethos, aims and objectives, and protecting the reputation of AAS.

Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other policies such as; AAS Child Protection & Safeguarding Policy, AAS Positive Relationships & Behaviour Policy & AAS Anti-Bullying Policy).

Scope

This policy applies to all members of the AAS community (including staff, scholars, LGC, volunteers, parents/carers and visitors) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their role.

The Education and Inspections Act 2006 empowers the Principal, to such extent as is reasonable, to regulate the behaviour of Scholars when they are off the 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 the Academy, but is linked to membership of the Academy. The Academy 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 the academy day.

Roles & Responsibilities

AAS is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, scholars, families and the reputation of AAS.

We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

This section outlines the roles and responsibilities for online safety of individuals and groups within the AAS.

Principal

Key responsibilities:

- Foster a culture of safeguarding where online safety is part of AAS holistic safeguarding approach
- Oversee the activities of the DSL and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- Liaise with the DSL on all online-safety issues which might arise and receive regular updates on Academy issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO (Data Protection Officer), DSL (Designated Safeguarding Lead) and LGC to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Will ensure the appropriate Filtering and Monitoring systems are in place within the Academy IT infrastructure.
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets the need of scholars, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure LGC are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the Academy website meets statutory requirements

Designated Safeguard Lead / Online Safety Lead

Key responsibilities (although the DSL can delegate certain online-safety duties, e.g. to the online safety coordinator, overall responsibility cannot be delegated; this assertion and all quotes below are from **Keeping Children Safe in Education 2023**):

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."
- Ensure "An effective approach to online safety [that] empowers an Academy or college to protect and educate the whole Academy or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with the local authority and work with other agencies in line with Working together to safeguard children"
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the Principal and DPO to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information

- Stay up to date with the latest trends in online
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others)
- Carry out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. KCSiE 2023 recommends the 360 Safe assessment tools:

  Risk Assessment: https://360safe.org.uk/overview/template-online-risk-assessment

  Self Assessment : https://360safe.org.uk

- Receive regular updates in online safety issues and legislation, be aware of local and Academy trends
- Ensure that online safety education is embedded across the curriculum and beyond, in wider Academy life
- Promote an awareness and commitment to online safety throughout the Academy community, with a strong focus on parents, who are often appreciative of Academy support in this area, but also including hard-to-reach parents
- Liaise with Academy technical, pastoral, and support staff as appropriate
- Communicate regularly with the wider SLT and the designated safeguarding committee member to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Ensure that the NetSupport DNA console is available on the devices of at least two members of the safeguarding team, and that there is a strategic plan to review and respond to triggers highlighted through NetSupport DNA.
- Ensure the 2021 DfE guidance on Sexual Violence and Harassment is followed throughout the Academy and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff.

Trust Network Manager and IT staff

The Network Manager is responsible for ensuring that (as listed in the 'all staff' section, plus):

- Keep up to date with the school's online safety policy and technical information to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead / data protection officer to ensure that Academy systems and networks reflect Academy policy
- Ensure all stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc)
- The Academy is equip the Academy with Sophos filtering software which includes a firewall that monitors and filters incoming and outgoing network traffic. Sophos' main purpose is to allow non-threatening digital traffic in and to keep potentially dangerous digital traffic out.
- Ensure appropriate levels of filtering are assigned to users by using the Sophos appliance
- The Academy is equip with NetSupport DNA monitoring software. NetSupport DNA will monitor the Academy network and identify when a user triggers terminology that could indicate potential harmful or risky behaviours.
- Maintain up-to-date documentation of the school's online security and technical procedures

- To report online safety related issues that come to their attention in line with Academy policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Monitor the use of Academy technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with Academy policy
- Work with the Principal to ensure the Academy website meets statutory DfE requirements

All staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) / Online Safety Lead (OSL) is
- Read and follow this policy in conjunction with the Academy Safeguarding Policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with academy procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy as directed on Athena.
- Notify the DSL if policy does not reflect practice and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all Academy activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise.
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in Academy or setting as homework tasks, encourage sensible use, monitor what scholars/Scholars are doing and consider potential dangers and the age appropriateness of websites
- To carefully supervise and guide Scholars when engaged in learning activities involving online technology (including, extra-curricular and extended Academy activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age-appropriate materials and signposting, and legal issues such as copyright and data law
- Prepare and check all online source and resources before using within the classroom
- Encourage scholars to follow their acceptable use policy, remind them about it and enforce Academy sanctions
- Notify the DSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL know
- Receive regular updates from the DSL and have a healthy curiosity for online safety issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the Academy hours and site, and on social media, in all aspects upholding the reputation of the Academy and of the professional reputation of all staff.

Assistant Principal for Personal Development

Key responsibilities (as listed in the 'all staff' section, plus):

- Embed consent, mental wellbeing, healthy relationships and staying safe online into the Personal Development curriculum and calendar. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their scholars' lives."
- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that scholars face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the Designated Safeguarding Lead and all other staff to ensure an understanding of the issues, approaches and messaging within Personal Development via CPD opportunities.

Computing department

Key responsibilities (as listed in the 'all staff' section, plus):

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in Academy to ensure a common and consistent approach, in line with acceptable-use agreements

Subject / Curriculum Leads

Key responsibilities (as listed in the 'all staff' section, plus):

- Look for opportunities to embed online safety in your subject or aspect, and model positive attitudes and approaches to staff and Scholars alike
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Ensure subject specific action plans also have an online safety element

Data Protection Officer

Key responsibilities (NB – this document is not for general data-protection guidance):

- Be aware of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document:
- "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without

consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children."

- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited
- Ensure general GDPR guidance is understood and followed by all stakeholders.

Volunteers and contractors

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the DSL as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology

Scholars (to an age-appropriate level)

Key responsibilities:

- Read, understand, sign and adhere to the scholar acceptable use policy and review this annually
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of Academy and realise that the school's acceptable use policies cover actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at Academy or outside Academy if there are problems

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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The Academy will therefore take opportunities to help parents understand these issues.

Key responsibilities:

- Read and countersign the scholar AUP (acceptable use policy if required) and ensure their children to follow it
- Consult with the Academy if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the Academy staff, volunteers, governors, contractors, Scholars or other parents/carers.

Community Users

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Support the Academy in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting

negative, threatening or violent comments about others, including the Academy staff, volunteers, governors, contractors, scholars or other parents/carers

Education and Training

The following subjects have the clearest online safety links:

- Art & Design
- ICT
- Tutor Sessions (Personal Development)

However, as stated above, it is the role of all staff to identify opportunities to thread online safety through all Academy activities, both outside the classroom and within the curriculum.

Equally, all staff should carefully supervise and guide scholars when engaged in learning activities involving online technology (including, extra-curricular and extended Academy activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age-appropriate materials and signposting, and legal issues such as copyright and data law.

At AAS we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World' from UKCIS (the UK Council for Internet Safety).

Annual reviews of curriculum plans / schemes of work (including for SEND scholars) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Acceptable Usage Policy

- Parents/carers will be required to read through and sign alongside their child's signature, helping to ensure their children understand the rules
- Staff and regular visitors to the Academy have an AUP that they must read through and sign to indicate understanding of the rules.

Copyright

- Scholars to be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations- staff to monitor this.
- Scholars are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- If using a search engine for images – staff / children should open the selected image and go to it's website to check for copyright.

Staff Training

- Online Safety Lead ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- A planned programme of online safety training is available to all staff. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the Academy Online Safety policy, Acceptable Usage and Child Protection Policies.
- The Online Safety Lead will receive regular updates through Local Authority and/or other information/training sessions and by reviewing guidance documents released.

- LCG representatives are invited to take part in online safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, online safety, health and safety or child protection.

Communication

Email:

- Digital communications with scholars (e-mail, online chat, VLE, voice etc.) should be on a professional level and only carried out using official Academy systems.
- 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, Academy curriculum systems);
- Under no circumstances should staff contact scholars, parents/carers or conduct any Academy business using personal e-mail addresses. If this happens by mistake, the DSL/Principal/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Academy e-mail is not to be used for personal use. Staff can use their own email in Academy (before, after Academy and during lunchtimes when not working with children) – but not for contact with parents/ scholars.
- If data needs to be shared with external agencies, this should be sent via the AnyComms System.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the Academy into disrepute or compromise the professionalism of staff.

Mobile Phones

- Academy mobile phones only should be used to contact parents/carers/scholars when on Academy business with scholars off site. Staff should not use personal mobile devices.
- Staff should not be using personal mobile phones in Academy during working hours when in contact with children.
- Scholars should adhere to the rules and guidelines set out in the Behaviour Policy regarding mobile phone use in school.

Social Networking Sites

Many social media platforms have a minimum age of 13, but the Academy regularly deals with issues arising on social media with scholars under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years

- Scholars will not be allowed to access social media/ networking sites at school.
- Staff should not access social networking sites on Academy equipment in Academy or at home. Staff should access sites using personal equipment.
- Staff users should not reveal names of staff, scholars, parents/carers or any other member of the Academy community on any social networking site or blog.
- Scholars/Parents/carers should be aware the Academy will investigate misuse of social networking if it impacts on the well-being of other scholars or stakeholders.
- If inappropriate comments are placed on social networking sites about the Academy or Academy staff then advice would be sought from the relevant agencies, including the police if necessary.

If parents have a concern about the school, we urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the Academy complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, scholars and parents, also undermining staff morale and the reputation of the Academy (which is important for the scholars and community that we serve).

Scholars are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Scholars are discouraged from 'following' staff, LGC, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). In the reverse situation, however, staff must not follow such public scholar accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Principal, and should be declared upon entry of the scholar or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Principal (if by a staff member).

Staff are reminded that they are obliged not to bring the Academy or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the Academy or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the Academy into disrepute.

The Academy has an active website and social media accounts which are used to inform and publicise Academy events as well as to celebrate and share the achievement of scholars.

Digital Images

The Academy record of parental permissions granted/not granted must be adhered to when taking images of our scholars.

Permissions are sought for:

- displays around the school
- the newsletter
- use in paper-based Academy marketing
- online prospectus or websites
- a specific high-profile image for display or publication
- social media

Under no circumstances should images be taken using privately owned equipment without the express permission of the Principal.

Where permission is granted the images should be transferred to Academy storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity. Images are stored on the Academy network in line with the retention schedule of the Academy Data Protection Policy.

Permission to use images of all staff who work at the Academy is sought on induction and a copy is located in the personnel file.

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose

Any scholars shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them)

Although many of the above points are preventative and safeguarding measures, it should be noted that the Academy will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information.

We encourage young people to think about their online reputation and digital footprint. Scholars are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children.

Scholars are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Scholars are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Removable Data Storage Devices

- Only encrypted USB devices are allowed write access. If not encrypted read access only.
- All files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using Academy provided anti-virus software before being run, opened or copied/moved on to local/network hard disks.
- Scholars should not bring their own removable data storage devices into Academy unless asked to do so by a member of staff.

Websites

- In lessons where internet use is pre-planned, scholars 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.
- Staff will preview any recommended sites before use.
- “Open” searches (e.g. “find images/ information on…”) are discouraged when working with younger scholars who may misinterpret information.
- 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.
- All users must observe copyright of materials published on the internet.
- Teachers will carry out a risk assessment regarding which scholars are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the scholars on the internet by the member of staff setting the task. All staff are aware that if they pass scholars working on the internet that they have a role in checking what is being viewed. Scholars are also aware that all internet use at Academy is tracked and logged.
- The Academy only allows the Online Safety Co-ordinator, Network Manager and SLT to access to Internet logs

Passwords

Staff:

- Passwords or encryption keys should not be recorded on paper or in an unprotected file
- Passwords should be changed at least every 3 months

- Users should not use the same password on multiple systems or attempt to “synchronise” passwords across systems

Scholars:

- Should only let Academy staff know their in-Academy passwords.
- Inform staff immediately if passwords are traced or forgotten. All staff are able to access the network to allow scholars to change passwords

Use of Own Equipment

- Privately owned ICT equipment should never be connected to the school’s network without the specific permission of the Principal or Network Manager.
- Scholars should not bring in their own equipment unless asked to do so by a member of staff.

Use of Academy Equipment

- No personally owned applications or software packages should be installed on to Academy ICT equipment;
- 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.
- All users should ensure any screens are locked (by pressing Ctrl, Alt, Del 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.

Monitoring

Keeping Children Safe in Education obliges schools to “ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”

All use of the school’s Internet access is logged, and the logs are randomly but regularly monitored by the school’s external provider. Whenever any inappropriate use is detected, it will be followed up by the Online Safety Lead, Scholar Managers, Progress Leaders or members of the Senior Leadership Team depending on the severity of the incident.

- Online Safety Lead and Network Manager will maintain the Change Control Log and record any breaches, suspected or actual, of the filtering systems
- Any member of staff employed by the Academy who comes across an online safety issue does not investigate any further but immediately reports it to the Online Safety Lead and impounds the equipment. This is part of the Academy safeguarding protocol. (If the concern involves the Online Safety Lead, then the member of staff should report the issue to the Principal).

Searching and confiscation

In line with the DfE guidance ‘Searching, screening and confiscation: advice for schools’, the Principal and staff authorised by them have a statutory power to search scholars/property on Academy premises. This includes the content of mobile phones and other devices, for example because of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying. All searches must be recorded using the Academy ‘Conducting a search’ documents and then handed to the Principal and uploaded to CPOMS.

Incident Reporting

It is vital that all staff recognise that online safety is a part of safeguarding and support this to be embedded into all areas of the Academy. Any online safety incidents which involve a member of staff must immediately be reported to the Principal (if a member of staff - unless the concern is about the Principal in which case the compliant is referred to the Head of Safeguarding as per the AAS Child Protection & Safeguarding Policy 2023.

Any online safety incidents regarding scholars should be reported on CPOMS.

The Academy will actively seek support from other agencies as needed (i.e. the local authority, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or scholars engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that scholars/scholars can come and talk to members of staff if they have made a mistake or had a problem in this area.

Sexting

It is important that everyone understands that whilst sexting is illegal, scholars/scholars can come and talk to members of staff if they have made a mistake or had a problem in this area. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

Responding to incidents of misuse

It is hoped that all members of the Academy 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.

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 will be dealt with accordingly.

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 Academy 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 Academy 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.

Appendix 1

The academy allows you to use computers and other devices to access the internet.

You are responsible for your behaviour and actions when accessing the internet in the academy.

It is important that all scholars take necessary measures to protect their own data from unauthorised access, damage, loss, abuse and theft.

All scholars have a responsibility to use the academy's computer system in a professional, lawful, and ethical manner.

To ensure that scholars are fully aware of their responsibilities when using ICT equipment and the academy systems. They are asked to read and sign this acceptable use policy.

Misuse of equipment, the internet and/or any form of electronic communication will result in you being denied use of this provision as well as further sanctions.

Acceptable Use

This applies to all academy devices and systems being used in the academy or at home.

I will

- Only access the academy's ICT systems and internet using my own username and password.
- Keep my password safe and not share it with other people.
- Report any materials or conduct which I feel is unacceptable and disturbing to a member of staff.
- Immediately report any ICT damage or faults to a member of staff.
- Only send emails to people I know or for further educational purposes e.g. applying for college courses etc.

I will not

- Damage academy ICT equipment on purpose.
- Download ICT viruses or malware.
- Log onto the computers using another person's details.
- Alter or delete another person's files.
- Impersonate another person by sending emails from their account.
- Search, download, upload or forward anything that is illegal or offensive to others.
- Open any attachments that I am unsure of.
- Take, publish, or share pictures or videos of anyone without their permission.
- Access inappropriate materials such as pornographic, racist or offensive material.
- Install or attempt to install or store programmes on any academy device.
- Try to alter computer settings.

I understand that the academy:

- Will monitor my use of the systems, devices and digital communications including emails, TEAMS and any other service that the academy provides.
- May share this information with my parents /carers, the police and/or other agencies depending upon the severity of the incident.
- May check my documents for viruses and unsuitable material at any time.

- Has the right to act against me if I am involved in an incident out of academy (examples would be cyber-bullying, use of images or personal information)

I understand that as a scholar at Astrea Academy Sheffield I:

- Am responsible for my actions, both in and out of the academy
- Must read and understand the above statements and agree to comply with the academy rules for use of ICT services
- Understand that failure to do this could result in the loss of my access rights to these services, along with further sanctions for serious misuse.

I have read and I understand the statements and I will follow the rules for the use of ICT services and the internet.	
Scholar Name:	**Scholar Signature:**
Date:	