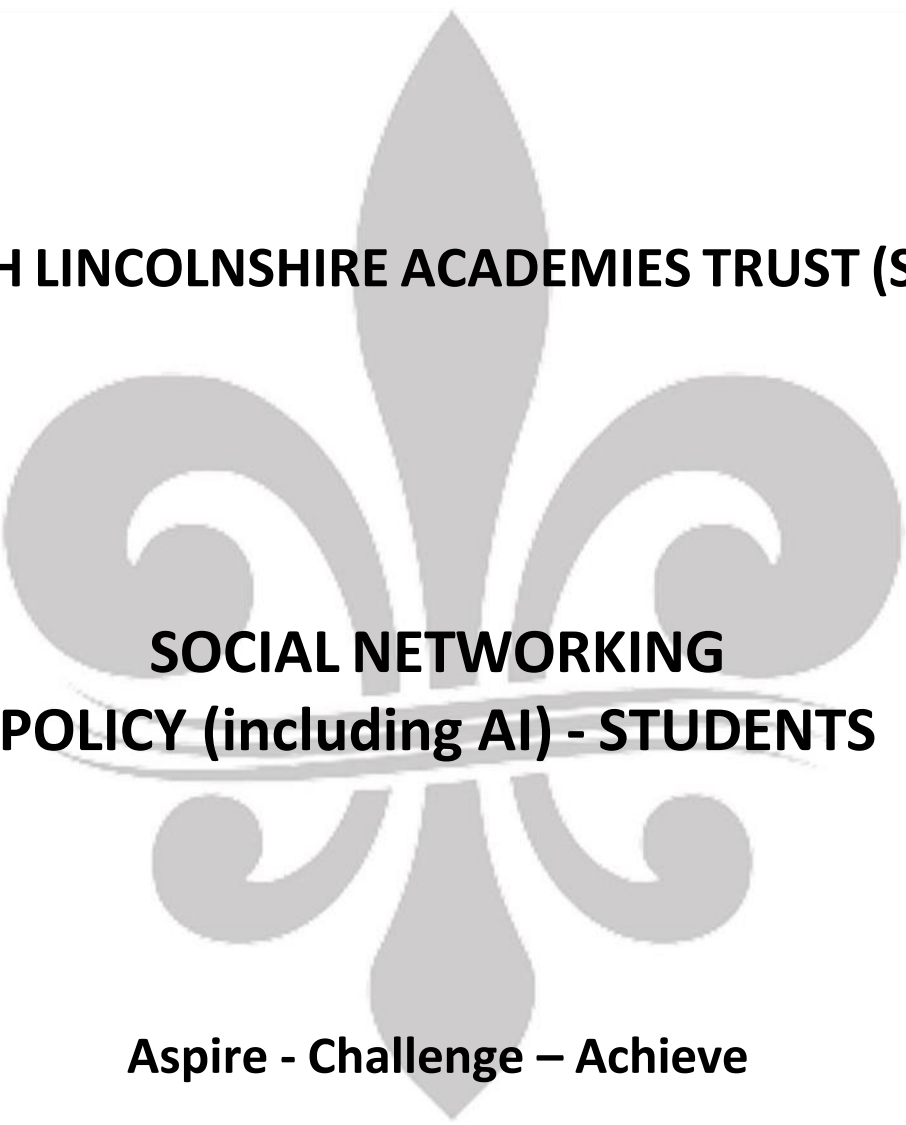




SOUTH LINCOLNSHIRE ACADEMIES TRUST (SLAT)

SOCIAL NETWORKING POLICY (including AI) - STUDENTS

Aspire - Challenge – Achieve

Owner	Approval	By Whom	Review
ARO/JCU	September 2026	Chief Executive Officer	Annually

INTRODUCTION

The Governing Body of South Lincolnshire Academies Trust is committed to ensuring that all students are aware of their responsibilities in connection with the growing use of social networking sites. It recognises that the use of such sites have become a very significant part of life for many people. They provide a positive way to keep in touch with friends and family, and can be used to exchange ideas and thoughts on common interests.

This policy will apply to ALL students attending South Lincolnshire Academy Trust schools.

WHAT IS A SOCIAL NETWORKING SITE?

‘A social network service focuses on building online communities of people who share interests and/or activities, or who are interesting in exploring the interests and activities of others. Most social network services are web-based and provide a variety of ways for users to interact, such as email and instant messaging services.

Social networking has encouraged new ways to communicate and share information. Social networking websites are being used regularly by millions of people.’

Any site that allows the interaction between people and/or organisations can be considered social networking, though most people think of Instagram, Snapchat or Facebook and similar sites as typical examples of social networking

AIMS

The policy aims to:

- Enable students to use social networking sites safely and securely;
- Ensure that students are aware of the risks associated with the inappropriate use of social networking sites;
- Ensure social media site are used positively and without negativity to school or individuals;
- Ensure any abuse/harassment online is dealt with effectively and in line with the school’s sanction system;
- Safeguard students in connection with the use of social networking sites and ensure they protect themselves from presenting as vulnerable;
- Ensure the Governing Body maintains its duty to safeguard children, the reputation of the School and the wider community.

LEGISLATION

The following legislation must be considered when adhering to this policy:

- Human Rights Act 1998;
- GDPR 2019 UK GDPR;
- Freedom of Information Act 2000;
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006;
- Regulation of Investigatory Powers Act 2000 (RIPA).

RESPONSIBILITIES

The Governing Body shall:

- Ensure this policy is implemented and procedures are in place that deal with the use of social networking sites;
- Ensure online safety is treated as part of the Trust's wider safeguarding arrangements, including risks linked to social media, online bullying, harmful content, AI generated content, image based abuse and online exploitation.
- Ensure that the policy reflects safe practice and that students are encouraged to use social networking in a positive and constructive fashion;
- Ensure appropriate filtering and monitoring systems are in place and that these are reviewed at least once every academic year by the senior leader responsible for filtering and monitoring, with support from the DSL and IT support.
- Ensure records are kept of filtering and monitoring checks, including what was checked, any concerns identified and the actions taken to resolve them.
- Ensure that all students have access to this policy and that new students are made aware of it.

The Chief Executive Officer (CEO), Deputy CEOs Senior Leadership Teams, Teaching and Support Staff shall:

- Be familiar with this policy and guidelines and ensure that employees understand the policy and their own responsibilities;
- Ensure that students are aware of the risks of the use of social networking sites and the possible implications of the inappropriate use of them;
- Instigate sanctions where appropriate to do so;
- Seek advice where necessary on the approach to be adopted if they are made aware of any potential issue.

Students shall:

- Behave responsibly at all times in connection with the use of social networking sites;
- Not post on social media other students photos, in uniform without their consent
- Operate safe practice when using social media;
- Ensure that any issues that occur are reported via the various support systems including the remote online support 'Worried@' on all school's website home pages;
- Co-operate with the school in ensuring the implementation of this policy.
- Not bring the school into disrepute on social media and will be asked to remove any posts which are deemed inappropriate.

USE OF SOCIAL NETWORKING SITES

For students' own security all communication via social networking sites should be made with the awareness that anything said, shown or received could be made available, intentionally or otherwise, to an audience wider than that originally intended. It is therefore, advised that students follow the following procedures:

- Students must not access social networking sites for personal use via school information systems or using school equipment;
- Students must not access social media platforms during the school day
- Students should not place inappropriate photographs or copy and distort images of school/staff or students on any social network space;
- Students should not make defamatory remarks about the Trust/staff or other students or post anything that could potentially bring the Trust into disrepute;
- Care should be taken to avoid using language which could be deemed as offensive to others.

In KS3, pupils 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

Pupils in KS4 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

By the end of secondary school, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviours apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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

USE OF AI

Generative artificial intelligence, often referred to as AI, is now widely available through apps, websites and online tools. This includes tools that can create text, images, audio, video, code and realistic content such as deepfakes.

The Trust recognises that AI can support learning when used appropriately, but it can also create safeguarding, bullying, privacy and plagiarism risks. Students must not use AI to impersonate another person, bully, harass, mislead, create harmful content, generate or alter images of another person without consent, or present AI generated work as their own.

Any use of AI that causes harm, distress, bullying, humiliation, discrimination, safeguarding concern or reputational damage will be treated seriously and managed in line with the Trust Behaviour Policy and safeguarding procedures. Where appropriate, the Trust may involve parents and carers, external agencies or the Police.

AI generated content must be age appropriate, lawful, accurate where relied upon for schoolwork, and used in a way that respects privacy, consent, copyright and the dignity of others. Students should not upload personal information, images, school data or information about another person into AI tools unless this has been clearly approved by school staff.

The Trust will teach students, through the curriculum and pastoral programme, how to use AI safely and responsibly. This will include understanding that AI can produce inaccurate or biased information, that AI generated images and deepfakes can cause significant harm, and that online behaviour is subject to the same expectations as behaviour in school.

We also recognise that AI has many uses to help pupils learn. For example:

- As a research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images

All AI-generated content must be properly attributed and appropriate for the pupils' age and educational needs.

AI may also lend itself to cheating and plagiarism. To mitigate this, pupils may not use AI tools:

- During assessments, including internal and external assessments, and coursework
- To write their homework or class assignments, where AI-generated text is presented as their own work
- To complete their homework, where AI is used to answer questions set and is presented as their own work (for example, maths calculations)

This list of AI misuse is not exhaustive. Students should ask a member of staff if they are unsure whether AI use is permitted for a particular piece of work or activity.

Where AI tools have been used as a source of information, pupils should reference their use of AI. The reference must show the name of the AI source and the date the content was generated.

Formal assessments

We will continue to take reasonable steps where applicable to prevent malpractice involving the use of generative AI in assessments. See our exams / assessment policy for more details.

SHARING NUDE OR SEMI NUDE IMAGES

The term sharing nude or semi nude images is used in this policy instead of sexting. This includes the taking, sending, receiving, possessing, storing, forwarding, uploading or sharing of nude or semi nude images, videos or AI generated images of a child or young person.

Students should never create, request, pressure another person to create, share, save, forward or threaten to share nude or semi nude images. This includes images created or altered using AI or image editing tools.

- take an explicit photo or video of themselves or a friend
- share an explicit image or video of a child, even if it's shared between children of the same age
- possess, download or store an explicit image or video of a child, even if the child gave their permission for it to be created.

Students across the Trust will be taught about the risks of sharing nude or semi nude images, including the impact on themselves and others, the importance of consent, the difficulty of removing images once shared, and the legal consequences of possessing or sharing indecent images of children. Students will also be reminded how to report concerns through school systems, including the DSL, pastoral team, trusted staff and Worried@ on school websites.

The Trust will take all reports involving nude or semi nude images seriously. Incidents will be managed as safeguarding concerns and investigated in line with the Trust's safeguarding, behaviour and child protection procedures.

Where there are concerns about exploitation, coercion, blackmail, harm, illegal imagery or wider safeguarding risk, the Trust will seek advice from or make referrals to appropriate safeguarding agencies or the Police.

The Trust will follow the guidelines set by the UK Council For Child Internet Safety:

Wherever possible, responses to incidents should be based on what safeguarding or pastoral leads have been told about the content, rather than staff viewing the imagery. Staff must not view, copy, save, forward, print or share nude or semi-nude images unless there is a clear and necessary safeguarding reason, agreed by the DSL, and recorded in line with safeguarding procedures. If illegal imagery is suspected, the image should not be viewed and advice should be sought from the Police or appropriate safeguarding agencies.

If a decision is made to view imagery the DSL would need to be satisfied that viewing:

- is the only way to make a decision about whether to involve other agencies (i.e. it is not possible to establish the facts from the young people involved)
- is necessary to report the image to a website, app or suitable reporting agency to have it taken down, or to support the young person or parent in making a report
- is unavoidable because a pupil has presented an image directly to a staff member or the imagery has been found on a school device or network. In line with Searching, Screening and Confiscation advice 2022

If it is necessary to view the imagery then the DSL should:

- Never copy, print or share the imagery; this is illegal.
- Discuss the decision with the Head of School (DSL) and DCEO for Safeguarding.
- Ensure viewing is undertaken by the DSL or another member of the safeguarding team with delegated authority from the Head of School.
- Ensure viewing takes place with another member of staff present in the room, ideally the Head of School or a member of the senior leadership team. This staff member does not need to view the images
- Wherever possible ensure viewing takes place on school premises, ideally in the Head of school or a member of the senior leadership team's office.
- Ensure wherever possible that images are viewed by a staff member of the same sex as the young person in the imagery
- Provide a written record of the viewing of the imagery in the school's safeguarding records including who was present, why the image was viewed and any subsequent actions. Ensure this is signed and dated and meets the wider standards set out by Ofsted for recording safeguarding incidents. Further details on searching, deleting and confiscating devices can be found in the DfE Searching, Screening and Confiscation advice 2020 (note this advice is for schools only). If youth produced sexual imagery has been unavoidably viewed by a member of staff either following a disclosure from a young person or as a result of a member of staff undertaking their daily role (such as IT staff monitoring school systems) then DSLs should ensure that the staff member is provided with appropriate support.

Viewing youth produced sexual imagery can be distressing for both young people and adults and appropriate emotional support may be required.

Deletion of images

If the Trust has decided that other agencies do not need to be involved, then consideration should be given to deleting imagery from devices and online services to limit any further sharing of the imagery. The Searching, Screening and Confiscation advice highlights that schools have the power to search pupils for devices, search data on devices and delete youth produced sexual imagery.'

BREACHES OF THIS POLICY

The Governing Body does not discourage students from using social networking sites. However, all students should be aware that the Governing Body will take seriously any occasions where the services are used inappropriately. If occasions arise of what could be deemed to be online bullying or harassment, these will be dealt with effectively and in line with the Trust sanction system (please see the Trust Behaviour Policy).

Under the Regulation of Investigatory Powers Act 2000 (RIPA), the Chief Executive Officer can exercise their right to monitor the use of the Trust's information systems and internet access where it is believed unauthorised use may be taking place; to ensure compliance with regulatory practices; to ensure standards of service are maintained; to prevent or detect crime, to protect the communication system and to pick up messages when someone is away from school.

If any instances of the inappropriate use of social networking sites are detected, depending on the seriousness of the allegations, action may be taken which could culminate in the student being excluded from the Trust.

There may be instances where the Trust will be obliged to inform the police of any activity or behaviour for which there are concerns as to its legality.