KIRTON ACADEMY

Online Safety Policy

Date reviewed:	**June 2024**	
Approved by:	**LGB**	**TBC**
Next review due by:	**Annually**	

For Office Use Only:

Policy Version: 1.0

To make changes to this policy, please email admin@lincolnshiregateway.co.uk.

Lincolnshire Gateway Academies Trust

Contents

1. Policy Aims

2.

This online safety policy has been written by Kirton Academy, involving staff, students and parents/carers, with specialist advice and input as required.

It takes into account the DfE statutory guidance "Keeping Children Safe in Education" 2023 and the North Lincolnshire Children's Multi Agency Resilience and Safeguarding (CMARS) procedures.

The purpose of Kirton Academy's online safety policy is to:

- Safeguard and protect all members of Kirton Academy community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

Kirton Academy identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

3. Policy Scope

Kirton Academy believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all students and staff are protected from potential harm online.
Kirton Academy identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
Kirton Academy believes that students should be empowered to build resilience and to develop strategies to manage and respond to risk online.
This policy applies to all staff including the Board of Trustees, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the Academy (collectively referred to as 'staff' in this policy) as well as students and parents/carers.
This policy applies to all access to the internet and use of technology, including personal devices, or where students, staff or other individuals have been provided with Academy issued devices for use off-site, such as a work laptops, tablets or mobile phones.

4. Links with other policies and practices

This policy links with a number of other policies, practices and action plans including:

- Anti-bullying Policy
- Acceptable Use Policy
- RRRR (Behaviour) Policy
- Safeguarding and Child Protection Policy

5. Monitoring and Review

Kirton Academy will review this policy at least annually

The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.

We will ensure that we regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

To ensure they have oversight of online safety, the Principal will be informed of online safety concerns, as appropriate.

The named Trustee for safeguarding will report on a regular basis to the Board of Trustees on online safety incidents, including outcomes.

Any issues identified will be incorporated into the Academy's action planning.

6. Roles and Responsibilities

The Academy has appointed Mrs K Ashwood, as Designated Safeguarding Lead to be the online safety lead.

Kirton Academy recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

The Senior Leadership Team (SLT) will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including an Acceptable Use Policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with technical staff to monitor the safety and security of Academy systems and networks.
- Ensure that online safety is embedded within a progressive whole Academy curriculum, which enables all students to develop an age-appropriate understanding of online safety.
- Support the Designated Safeguarding Lead by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the Academy community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology. Audit and evaluate online safety practice to identify strengths and areas for improvement.

The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the Academy community, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the Academy's safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the Principal and Board of Trustees.
- Work with the SLT to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet termly with the Trustee with a lead responsibility for safeguarding and online safety.

- Meet fortnightly with Year Leaders to discuss all aspects of safeguarding including online safety.

It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and Acceptable Use Policy
- Take responsibility for the security of Academy systems and the data they use, or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the Academy's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and SLT, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures *(including password policies and encryption)* to ensure that the Academy's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the Academy's filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the SLT.
- Report any filtering breaches to the DSL and SLT, as well as, the Academy's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the Academy's safeguarding procedures.

It is the responsibility of students (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age-appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the Academy's online safety guidance in student journal
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

It is the responsibility of parents and carers to:

- Read the Academy online safeguarding information published on the Academy website and encourage their children to adhere to them.
- Support the Academy in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the Academy, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Use Academy systems and other network resources safely and appropriately.

- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

7. Education and Engagement Approaches

Education and engagement with students

The Academy will establish and embed a progressive online safety curriculum throughout the whole Academy, to raise awareness and promote safe and responsible internet use amongst students by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in the PSHE, SRE and Computing programmes of study, covering use both at home and Academy.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating students in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The Academy will support students to read and understand the Acceptable Use Policy in a way which suits their age and ability by:

- Informing students that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Rewarding positive use of technology by students.
- Implementing appropriate peer education approaches.
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Seeking student voice when writing and developing Academy online safety policies and
  practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support the Academy's internal online safety education approaches.

Vulnerable Students

Kirton Academy is aware that some students are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

Kirton Academy will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable students. This will include students accessing the Indigo provision.

Kirton Academy will seek input from specialist staff as appropriate, including the SENCO (Mrs S Palin) and the Designated Teacher for Looked After Children (Mrs K Ashwood)

Training and engagement with staff

The Academy will:

- Provide and discuss the online safety policy with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates as part of existing safeguarding and child protection training/updates. This will cover the potential risks posed to students (Content, Contact and Conduct) as well as our professional practice expectations.

- Make staff aware that Academy systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with Academy's policies when accessing Academy systems and devices.
- Make staff aware that their online conduct out of Academy, including personal use of social media, could have an impact on their professional role and reputation within Academy.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the students.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting students, colleagues or other members of the Academy community.

Awareness and engagement with parents and carers
Kirton Academy recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.

The Academy will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness information via the Academy website and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days as appropriate:
- Drawing their attention to the Academy online safety policy and expectations in letters, our prospectus and on our website;
- Requesting that they read online safety information as part of joining our Academy, for example, within our student journal and on Academy website

8. Reducing Online Risks

Kirton Academy recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:

- Regularly review the methods used to identify, assess and minimise online risks;
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the Academy is permitted;
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material;
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a Academy computer or device;

All members of the Academy community are made aware of the Academy's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the Academy's Acceptable Use Policy and highlighted through a variety of education and training approaches.

9. Safer Use of Technology

Classroom Use
Kirton Academy uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Academy learning platform/web-based subject learning
- Email
- Digital cameras and video cameras
- Online learning – MS Teams

All Academy owned devices will be used in accordance with the Academy's Acceptable Use Policy and with appropriate safety and security measures in place.

Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

The Academy will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.

The Academy will ensure that the use of internet-derived materials, by staff and students, complies with copyright law and acknowledge the source of information.

Supervision of students will be appropriate to their age and ability:

Key Stage 3 and 4 - Students will be appropriately supervised when using technology, according to their ability and understanding.

Managing Internet Access

- The Academy will maintain a written record of users who are granted access to the Academy's devices and systems.
- All staff will read and sign an Acceptable Use Policy and Parents must complete and sign an online permissions form to enable students to access the internet before being given access to the Academy computer system, IT resources or internet.

Filtering and Monitoring

Decision Making

Kirton Academy Trustees and leaders have ensured that the Academy has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks. The Trustees and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.

The Academy's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our Academy's specific needs and circumstances. Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the SLT. The SLT will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard students; effective classroom management and regular education about safe and responsible use is essential.

Filtering

The Academy uses educational broadband connectivity through Entanet International Ltd, in conjunction with Talk Talk.

The Academy uses WatchGuard filtering to block sites which can be categorised as: pornography, racial hatred, extremism, gaming, social media and sites of an illegal nature.

The Academy works with Watch Guard to ensure that our filtering policy is constantly updated.

The Academy continually monitors the use of bad language/inappropriate internet searching.

Dealing with Filtering breaches

- The Academy has a clear procedure for reporting filtering breaches.
- If students discover unsuitable sites, they will be required to report it immediately to a member of staff.

- The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead and/or technical staff.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.

Any material that the Academy believes is illegal will be reported immediately to the appropriate agencies.

Monitoring
The Academy will appropriately monitor internet use on all Academy owned or provided internet enabled devices. This is achieved by:

- Physical monitoring (supervision);
- Monitoring internet and web access (reviewing logfile information)
- Pro-active technology monitoring services.

The Academy has a clear procedure for responding to concerns identified via monitoring approaches. DSL will respond in line with the Safeguarding and child protection policy.
All users will be informed that use of Academy systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

Managing Personal Data Online
Personal data will be recorded, processed, transferred and made available online in accordance with the GDPR legislation.

Security and Management of Information Systems
The Academy takes appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on the Academy's network,
- The appropriate use of user logins and passwords to access the Academy network.
- Specific user logins and passwords will be enforced for all members of the Academy community
- All users are expected to log off or lock their screens/devices if systems are unattended.

Password policy
All members of staff will have their own unique username and private passwords to access Academy systems; members of staff are responsible for keeping their password private.
From entry into year 7, or at date of admission for in-year transfers, all students are provided with their own unique username and private passwords to access Academy systems; students are responsible for keeping their password private.

We require all users to:

- Use strong passwords for access into our system.
- Change their passwords when prompted.
- Always keep their password private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.

Managing the Safety of the Academy Website
The Academy will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).

The Academy will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.

Staff or students' personal information will not be published on our website; the contact details on the website will be the Academy address, email and telephone number.
The administrator account for the Academy website will be secured with an appropriately strong password.

The Academy will post appropriate information about safeguarding, including online safety, on the Academy website for members of the community.

Publishing Images and Videos Online
The Academy will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to): Acceptable Use, Codes of conduct, Social media and Use of personal devices and mobile phones.

Managing Email

- Access to Academy email systems will always take place in accordance with Data protection legislation and in line with other Academy policies, including: Acceptable Use Policy and Safeguarding and Child Protection Policy.
- The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- Academy email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the Academy community will immediately tell Mrs C Ireland (Network Manager) if they receive offensive communication.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked in Academy.

Staff

- The use of personal email addresses by staff for any official Academy business is not permitted.
- All members of staff are provided with a specific Academy email address, to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and students and parents.

Students

- Students will use Academy provided email accounts for educational purposes.
- Students will sign a home-Academy agreement in the Academy journal, read the mobile and internet safety information provided and will receive education regarding safe and appropriate email etiquette before access is permitted.

Management of Learning Platforms
Kirton Academy uses Office 365 as its official learning platform.

Leaders and staff will regularly monitor the usage of Office 365 in all areas, in particular, message and communication tools and publishing facilities.

Only current members of staff and students will have access to Office 365

When staff and/or students leave the Academy, their account or rights to specific Academy areas will be disabled or transferred to their new establishment on request.

Students and staff will be advised about acceptable conduct and use when using Office 365.

All users will be mindful of copyright and will only upload appropriate content onto Office 365 following appropriate training.

Any concerns about content on Office 365 will be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- If the user does not comply, the material will be removed by the network manager, the account will be disabled or removed.
- Access to Office 365 for the user may be suspended.
- The user will need to discuss the issues with a member of the SLT before reinstatement. A student's parent/carer may be informed.
- If the content is considered to be illegal, then the Academy will respond in line with existing child protection procedures.

A visitor may be invited to use Office 365 by a member of the SLT; in this instance, there may be an agreed focus or a limited time slot. A valid Academy email account will be required in order to access Office 365.

Management of Applications (apps) used to Record Children's Progress
The Academy uses SIMS and SMID to track students' progress and shares appropriate information with parents and carers.

The Principal is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation

In order to safeguard students' data:

- Academy issued devices are used for apps that record and store children's personal details, attainment or photographs.
- Access to student data for staff is secure and password protected.
- Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
- School devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

Social Media

Expectations
The expectations regarding safe and responsible use of social media applies to all members of Kirton Academy community.

The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.

All members of Kirton Academy community are expected to engage in social media in a positive, safe and responsible manner, at all times.

All members of Kirton Academy community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

The Academy will control student and staff access to social media whilst using Academy provided devices and systems on site.

The use of social media during Academy hours for personal use is not permitted.

Inappropriate or excessive use of social media during Academy/work hours or whilst using School devices may result in disciplinary or legal action and/or removal of internet facilities.

Concerns regarding the online conduct of any member of Kirton Academy community on social media, should be reported to the Academy and will be managed in accordance with our Anti-bullying, Allegations against staff, Behaviour and Safeguarding policies.

Staff Personal Use of Social Media
The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the Academy Code of conduct within the Acceptable Use Policy.

Reputation
All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within Academy. Disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Setting the privacy levels of their personal sites as strictly as they can.
- Being aware of location sharing services.
- Opting out of public listings on social networking sites.
- Logging out of accounts after use.
- Keeping passwords safe and confidential.
- Ensuring staff do not represent their personal views as that of the Academy.
- Members of staff are encouraged not to identify themselves as employees of Kirton Academy on their personal social networking accounts. This is to prevent information on these sites from being linked with the Academy and also to safeguard the privacy of staff members.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with Academy's policies and the wider professional and legal framework.

Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members or colleagues will not be shared or discussed on social media sites.

Members of staff will notify the SLT immediately if they consider that any content shared on social media sites conflicts with their role in the Academy.

Communicating with students and parents and carers
All members of staff are advised not to communicate with or add as 'friends' any current or past students or current or past students' family members via any personal social media sites, applications or profiles.

Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the Principal.

If ongoing contact with students is required once they have left the Academy roll, members of staff will be expected to use existing alumni networks or use official Academy provided communication tools.

Staff will not use personal social media accounts to contact students or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Principal.

Any communication from students and parents received on personal social media accounts will be reported to the Academys Designated Safeguarding Lead.

Students' Personal Use of Social Media
Safe and appropriate use of social media will be taught to students as part of an embedded and progressive education approach, via age appropriate sites and resources.

The Academy is aware that many popular social media sites state that they are not for children under the age of 13, therefore the Academy will not create accounts specifically for children under this age.

Any concerns regarding students' use of social media, both at home and at Academy, will be dealt with in accordance with existing Academy policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

Students will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, Academy attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications and report concerns both within Academy and externally.

Official Use of Social Media
Kirton Academy official social media channels are:

- Facebook
- Twitter
- Instagram

The official use of social media sites, by the Academy, only takes place with clear educational or community engagement objectives, with specific intended outcomes.
The official use of social media as a communication tool has been formally risk assessed and approved by the Principal.

Leadership staff have access to account information and login details for the social media channels, in case of emergency, such as staff absence.

Official Academy social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
Staff use Academy provided email addresses to register for and manage any official Academy social media channels.

Official social media sites are suitably protected and, where possible, are linked to the Academy website.

Public communications on behalf of the Academy will, where appropriate and possible, be read and agreed by at least one other colleague.

Official social media use will be conducted in line with existing policies, including: Anti-bullying, Photo permissions, Data protection and Safeguarding.

All communication on official social media platforms will be clear, transparent and open to scrutiny.

Parents, carers and students will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
Social media tools which have been risk assessed and approved as suitable for educational purposes will be used.

Any official social media activity involving students will be moderated by the Academy where possible.

Parents and carers will be informed of any official social media use with students and written parental consent will be obtained, as required.

The Academy will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations
Members of staff who follow and/or like the Academy social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

If members of staff are participating in online social media activity as part of their capacity as an employee of the Academy, they will:

- Sign the Academy's Acceptable Use Policy.
- Be professional at all times and aware that they are an ambassador for the Academy.
- Disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the Academy.
- Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace, including: Libel, Defamation, Confidentiality, Copyright, Data protection and Equalities laws.
- Ensure that they have appropriate written consent before posting images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the Academy unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, students, parents and carers.

- Inform their line manager, the Designated Safeguarding Lead and/or the Principal of any concerns, such as criticism, inappropriate content or contact from students.

Use of Personal Devices and Mobile Phones

Kirton Academy recognises that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents/carers, but technologies need to be used safely and appropriately within Academy.

Expectations
All use of personal devices and mobile phones will take place in accordance with the law and other appropriate Academy policies, including, but not limited to: Mobile Phone Policy (copy in student journal), Anti-bullying, RRR Behaviour and Safeguarding and Child Protection.

Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.

All members of Kirton Academy community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the Academy accepts no responsibility for the loss, theft or damage of such items on Academy premises.

All members of Kirton Academy community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our RRRR (Behaviour) policy.

All members of Kirton Academy community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the Academy Behaviour or Safeguarding policies.

Staff Use of Personal Devices and Mobile Phones
Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant Academy policy and procedures, such as: Confidentiality, Safeguarding, Data security and Acceptable use.

Staff will be advised to:

- Keep mobile phones and personal devices in a safe and secure place during lesson time
- Keep mobile phones and personal devices switched off or switched to ‘silent’ mode during lesson times.
- Ensure that Bluetooth or other forms of communication (such as ‘airdrop’) are hidden or disabled during lesson times.
- Not use personal devices during teaching periods, unless written permission has been given by the Principal, such as in emergency circumstances.
- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

Members of staff are not permitted to use their own personal phones or devices for contacting students or parents and carers.

Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Lead and/or Principal.

If a member of staff breaches the Academy policy, action will be taken in line with the Academy behaviour and allegations policy

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, appropriate action will be taken.

Students' Use of Personal Devices and Mobile Phones
Students will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

Kirton Academy expects student's personal devices and mobile phones to be switched off and kept out of sight during the School day.

If a student needs to contact his/her parents or carers they will go to their Year Leader or Reception and will be allowed to use a Academy phone.

Parents are advised to contact their child via Reception or their Year Leader during Academy hours; exceptions may be permitted on a case-by-case basis, as approved by the Principal.

Mobile phones or personal devices will not be used by students during lessons or formal Academy time.

Mobile phones and personal devices must not be taken into examinations.

Students found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

If a student breaches the Academy policy, the phone or device will be confiscated and will be held at Reception.

Academy staff may confiscate a student's mobile phone or device if they believe it is being used to contravene the Academy's Behaviour or Anti-Bullying policy, or could contain youth produced sexual imagery (sexting).

Searches of mobile phone or personal devices will only be carried out in accordance with the Academy's policy.

Students' mobile phones or devices may be searched by a member of the SLT, with the consent of the student or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes Academy policies. **This is not the case when images of a sexual nature may be present on the phone.**

Mobile phones and devices that have been confiscated will be released to students at the end of the School day on the first occasion. On the second occasion, they will be returned following a discussion with parent/carer, and on the third occasion the phone or device will need to be collected from Academy by the parent/carer.

If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, legal advice will be sought and the device may be handed over to the police for further investigation.

Visitors' Use of Personal Devices and Mobile Phones
Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the Academy's Acceptable Use Policy and other associated policies, such as: Anti-bullying, Behaviour and Safeguarding.

The Academy will ensure appropriate information is provided to inform parents, carers and visitors of expectations of use.

Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of Academy policy.

Responding to Online Safety Incidents and Concerns

All members of the Academy community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), sexual violence, sexual harassment, cyberbullying and illegal content.

All members of the community must respect confidentiality and the need to follow the official Academy procedures for reporting concerns.

Students, parents and staff will be informed of the Academy's complaints procedure and staff will be made aware of the whistleblowing procedure.

The Academy requires staff, parents, carers and students to work in partnership to resolve online safety issues.
After any investigations are completed, the Academy will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

If the Academy is unsure how to proceed with an incident or concern, the DSL will seek advice from the North Lincolnshire CMARS.

Where there is suspicion that illegal activity has taken place, the Academy will contact the North Lincolnshire CMARS or Police using 101, or 999 if there is immediate danger or risk of harm.

If an incident or concern needs to be passed beyond the Academy community (for example if other local Academys are involved or the public may be at risk), the Academy will speak with Police and/or the North Lincolnshire CMARS first, to ensure that potential investigations are not compromised.

Concerns about Students Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
- The DSL will record these issues in line with the Academy's safeguarding policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the North Lincolnshire CMARS thresholds and procedures.
- The Academy will inform parents and carers of any incidents or concerns involving their child, as and when required.

Staff Misuse

Any complaint about staff misuse will be referred to the Principal.

Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).

Appropriate action will be taken in accordance with the Behaviour policy and Code of conduct.

Procedures for Responding to Specific Online Incidents or Concerns

Youth Produced Sexual Imagery or "Sexting", Sexual Violence and Sexual Harassment

Kirton Academy recognises youth produced sexual imagery (known as "sexting"), sexual violence and sexual harassment as a safeguarding issue; therefore, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

The Academy will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in Academys and colleges: responding to incidents and safeguarding young people' and North Lincolnshire CMARS guidance, as well as the OFSTED review on Sexual Abuse in Academys 2021.

Kirton Academy will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting', sexual violence and sexual harassment by implementing preventative approaches, via a range of age and ability appropriate educational methods including curriculum lessons, assemblies and small-group work as applicable.

The Academy will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery, sexual violence and sexual harassment.

Dealing with 'Sexting'
If the Academy are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the Academy will:

- Act in accordance with our Safeguarding policy and the relevant North Lincolnshire CMARS procedures.
- Immediately notify the Designated Safeguarding Lead.
- Store the device securely.
- If an indecent image has been taken or shared on the Academy network or devices, the Academy will act to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of student(s) involved; including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Make a referral to Specialist Children's Services and/or the Police, as appropriate.
- Provide the necessary safeguards and support for students, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with the Academy's Behaviour policy, but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in Academys and colleges: responding to incidents and safeguarding young people' guidance.
- Images will only be deleted once the Academy has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.
- The Academy will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off Academy premises, using Academy or personal equipment.

The Academy will not:

- View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
- In this case, the image will only be viewed by the Designated Safeguarding Lead and their justification for viewing the image will be clearly documented.
- Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request students to do so.

Online Child Sexual Abuse and Exploitation including Sexual Violence and Sexual Harassment
Kirton Academy will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

Kirton Academy recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

The Academy will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for students, staff and parents/carers.

The Academy will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally. (Academy website).

Dealing with Online Child Sexual Abuse and Exploitation including Sexual Violence and Sexual Harassment
If the Academy are made aware of incident involving online sexual abuse of a child, the Academy will:

- Act in accordance with the Academy's Safeguarding policy and the relevant North Lincolnshire CMARS procedures.
- Immediately notify the Designated Safeguarding Lead.
- Store any devices involved securely.
- Immediately inform police via 101 (or 999 if a child is at immediate risk)
- Carry out a risk assessment which considers any vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Make a referral to Specialist Children's Services (if required/ appropriate).
- Provide the necessary safeguards and support for students, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; Academy leadership team will review and update any management procedures, where necessary.

The Academy will take action regarding online child sexual abuse, regardless of whether the incident took place on/off Academy premises, using Academy or personal equipment.

Where possible students will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report : www.ceop.police.uk/safety-centre/

If the Academy is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the North Lincolnshire CMARS or local police.

If the Academy is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the relevant authorities by the Designated Safeguarding Lead.

If students at other Academys are believed to have been targeted, the Academy will seek support from local Police and/or the North Lincolnshire CMARS first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)
Kirton Academy will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

The Academy will take action regarding IIOC on Academy equipment and/or personal equipment, even if access took place off site.

The Academy will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software. This is currently Watch Guard and Microsoft Essentials.

If the Academy is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through local Police and/or the North Lincolnshire CMARS.

If made aware of IIOC, the Academy will:

- Act in accordance with the Academy's safeguarding policy and the relevant North Lincolnshire North Lincolnshire CMARS procedures.
- Immediately notify the Academy Designated Safeguard Lead.
- Store any devices involved securely.
- Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), local police or the LADO.

If made aware that a member of staff or a student has been inadvertently exposed to indecent images of children whilst using the internet, the Academy will:

- Ensure that the Designated Safeguard Lead is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the School devices, the Academy will:

- Ensure that the Designated Safeguard Lead is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.

If made aware that a member of staff is in possession of indecent images of children on School devices, the Academy will:

- Ensure that the Principal is informed.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the Academy's managing allegations policy.
- Quarantine any devices until police advice has been sought.

Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at Kirton Academy. Full details of how the Academy will respond to cyberbullying are set out in the Anti-bullying policy which is available on the Academy website. Key advice is also published in the student journal.

Online Hate

Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Kirton Academy and will be responded to in line with existing Academy policies, including Anti-bullying and Behaviour.

All members of the community will be advised to report online hate in accordance with relevant Academy policies and procedures.

The Police will be contacted if a criminal offence is suspected.

If the Academy is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the North Lincolnshire CMARS and/or local police.

Online Radicalisation and Extremism
The Academy will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in Academy.

If the Academy is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Safeguarding policy.

If the Academy is concerned that member of staff may be at risk of radicalisation online, the Principal will be informed immediately and action will be taken in line with the Safeguarding and Inclusion policies.

Useful Links for Educational Settings

North Lincolnshire CMARS - http://www.northlincscmars.co.uk/

A guide for education settings about establishing 'appropriate levels' of filtering and monitoring can be found at: https://www.saferinternet.org.uk/advice-centre/teachers-and-Academy-staff/appropriate-filtering-and-monitoring

National Links and Resources

Action Fraud: www.actionfraud.police.uk

CEOP:
www.thinkuknow.co.uk
www.ceop.police.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF): www.iwf.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

NSPCC: www.nspcc.org.uk/onlinesafety

ChildLine: www.childline.org.uk
Net Aware: www.net-aware.org.uk

The Marie Collins Foundation: www.mariecollinsfoundation.org.uk

UK Safer Internet Centre: www.saferinternet.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

360 Safe Self-Review tool for Schools: www.360safe.org.uk