Kingsley Academy
Policy for E-Safety

Approved by: Helen Darby	**Date: 09/06/2025**
Last reviewed on:	
Next review due by: 09/06/2026	
Governor Approved by: LSingh	

Statement of Intent

Kingsley Academy is an alternative provision which accepts children from 14-16 years. The academy plays a significant part in the prevention of harm to our students through its human-centred approach. The emotional well-being of our students is central to this approach. Children can feel safe and be themselves, and relationships are valued and nurtured in a culture of mutual respect. The academy believes it is the responsibility of all members of the learning community, including children, staff and parents, to uphold this culture and to work towards ensuring that we can all learn together in a safe environment free from fear. We recognise that this ethos of care is as relevant to online experiences as it is in other aspects of our lives. This policy should be read in conjunction with our Safeguarding Policy, Behaviour Anti-Bullying Policy, ICT, Social networking policy, Internet policy and preventing extremism & radicalisation policy

The purpose of this policy is to:

- Set out the key principles expected of all members of the learning community with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist academy staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole learning community.
- Have clear structures to deal with online abuse such as online-bullying.
- Ensure that all members of the learning community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our learning community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and wellbeing (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope of the Policy

This policy applies to all members of the learning community (including staff, students, volunteers, parents / carers, visitors, contractors, community users) who have access to and are users of school ICT systems, both in and out of the school. The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online- bullying, or other online-safety incidents covered by this policy, which may take place outside of the academy, but are linked to membership of the academy. The school will respond to incidents of inappropriate online-safety behaviour that take place outside of school in line with its Behaviour and Anti-bullying Policies.

Online-safety Group

The Online-safety Group provides a consultative group that meets to monitor and review the Online-safety Policy and in response to need. Members of the Online-safety Group include the E Safety Co-ordinator, Designated Safeguarding Officer Safeguarding Governor and students

Roles & Responsibilities

As E- Safety is an important aspect of strategic leadership within the academy, the Head has ultimate responsibility to ensure that the policy and practices are embedded and monitored.

This policy, supported by the school's acceptable use agreements for staff, IEB, visitors and students, is to protect the interests and safety of the whole school community.

Head Teacher and Senior Leaders:

• The Headteacher is responsible for ensuring the safety (including e-safety) of members of the learning community, though the day-to-day responsibility for e- safety

• The Headteacher / Senior Leaders are responsible for ensuring that relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues.

• The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in the academy who carry out the internal safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

E-Safety Coordinator:

- Has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff
- Liaises with school ICT technical staff
- Receives reports of e-safety incidents and creates a log of incidents
- Meets with online safety group to discuss current issues.

Technical Staff

- The academy meets the e-safety technical requirements outlined in the Acceptable Usage Policy.
- The Internet provider is informed of any issues relating to the filtering applied by the Internet provider Policy central supplied by future
- Monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff:

• They have an up-to-date awareness of e-safety matters and of the current school e-safety policy and practices.

• They have read, understood and signed the school Staff Acceptable Use Policy Agreement (AUP).

• They report any suspected misuse or problem to the E-Safety Coordinator /Headteacher

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

• They are aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices.

Students:

• Use the academy's ICT systems in accordance with the Student Acceptable Use Policy, which they need to accept each time they log on to the school network.

• Have a good understanding of research skills and the copyright regulations

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

• Will be expected to know and understand academy policies on the use of mobile phones, digital cameras and handheld devices.

. They should also know and understand academy policies on the taking / use of images and on cyber-bullying.

• Understand the importance of adopting good e-safety practice when using digital technologies out of school.

Parents / Carers:

The academy works closely with parents and guardians. We will always contact parents with any concerns and hope that parents will share their concerns with the academy.

The academy recognises that not all parents feel equipped to protect their child when they use electronic equipment at home. The academy will therefore take every opportunity to help parents understand these issues through coffee mornings, parents' evenings, letters, Information on the academy website.

Staff and Volunteer Training

The academy ensures all teaching staff receive regular, up-to-date online-safety training to carry out their responsibilities as outlined in this policy.
An introduction to safeguarding, online safety and the acceptable use of ICT is offered as part of the induction programme for all new staff and volunteers.

Online safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-Safety guidance to be given to the students on a regular and meaningful basis. E-Safety is embedded within our curriculum, and we continually look for new opportunities to promote E-Safety.

- The academy has a framework for teaching internet skills in Computing/ICT lessons
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Students are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities
- Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or the'CEOP report abuse' button
- They are taught to evaluate the integrity of different sources and to recognise that some websites that appear to be impartial may be sources of propaganda (including e.g. racist, homophobic or extremist views).

Responding to Online –Safety Incidents

The academy takes all reasonable steps to ensure online-safety and communicates this policy to staff, students and parents. Monitoring and reporting of online safety incidents take place and contributes to developments in policy and practice in online-safety within the academy. There may be times when

infringements of the policy could take place through careless, irresponsible or through deliberate misuse. In this instance the academy will:

- Require that any suspected online risk or infringement is reported to Headteacher, Safeguarding officers or E-safety co-ordinator due to the nature of the incident that day.
- Ensure that issues are dealt with quickly, sensitively and in a proportionate manner, through the school's escalation processes: *Safeguarding, Behaviour, Complaints, Discipline* and *Whistleblowing Procedures.*
- Actively seek support from other agencies as needed (i.e. the local authority,
- UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police) in dealing with online safety issues.
- Informed parents/ carers of online safety incidents involving young people for whom they are responsible.
- Contact the Police if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law.
- Immediately refer any suspected illegal material to the appropriate authorities (Police and Internet Watch Foundation).
- Any concerns about staff misuse are always referred directly to the Headteacher, unless the concern is about the Head teacher in which case the complaint is referred to the Chair of IEB. Concerns will then be referred to the LADO (Local Authority's Designated Officer).

Managing ICT Systems & Devices

The academy is responsible for ensuring that the ICT network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. This includes ensuring that academy technical systems are managed in ways that meet recommended technical requirements and regular reviews and audits of the safety and security of academy technical systems are undertaken.

The ICT Network

All users have clearly defined access rights to academy ICT systems:

- All staff and students are provided with a username and secure password. Users are responsible for the security of their username and password
- A "Guest" login is provided for temporary access for e.g. supply teachers and visitors onto the school systems.
- The ICT Technician maintains an up-to-date record of users and their usernames.
- Users are asked to log out of systems when leaving their computer and there is an automatic lock-out for staff after 10 minutes' idle time.
- All servers are password protected and managed by DBS-checked staff. Users report any actual or potential incident or security breach to the

Headteacher.

- Appropriate security measures are in place to protect school ICT infrastructure (including anti-virus software, firewalls and internet filtering software).
- Personal or sensitive data is only stored on the school's secure network or on password-protected devices. Staff are responsible for ensuring the safe, secure use of removable media (e.g. memory sticks / CDs / DVDs) on academy devices.
- All Staff are provided with an encrypted USB for confident information Filters & Monitoring
-
- Appropriate precautions are in place to ensure students are not exposed to inappropriate online material, but we acknowledge the need to teach students how and why to behave responsibly in order to protect themselves. School Internet access is controlled through policy central from Future

- Our academy also employs some additional web-filtering, which is the responsibility of Wolverhampton Council.

- Kingsley Academy is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998

- Staff and students are aware that academy-based email and internet activity can be monitored and explored further if required

- If staff or students discover an unsuitable site, the screen must not be switched off/ closed and the incident reported immediately to the e- safety coordinator or teacher as appropriate

- **Managing Other Online Technologies**
- Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavors to deny access to social networking and online games websites to students within school

- All students are advised to be cautious about the information given by others on such websites, for example users not being who they say theyare

- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider

the appropriateness of any images they post due to the difficulty of removing an image once online

- Students are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)

- Our students are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals

- Students are encouraged to be wary about publishing specific and detailed private thoughts and information online

- Our students are asked to report any incidents of Cyberbullying to the academy.

- **Parental Involvement**

- We believe that it is essential for parents/carers to be fully involved with promoting E-Safety both in and outside of the academy and to be aware of their responsibilities. We regularly consult and discuss E-Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the academy

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on academy website)

- The academy disseminates information to parents relating to ESafety where appropriate in the form of;

    - Parents evenings
    - Posters
    - Academy website information
    - Newsletter items
- Mobile Technologies

- Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such Smart phones, iPads, games players, are generally very familiar to children outside of academy. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use.
- Emerging technologies will be examined for educational benefit and the risk

assessed before use in school is allowed. Our academy chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices

- For the safety of all on site, mobile phones are not to be accessed in the main body of the academy. If there are any specific issues individual staff members need to see the Headteacher.
- Students are allowed to bring personal mobile devices/phones to the academy but hand them in when they arrive at the academy then handed back at the end of the school day
- The academy is not responsible for the loss, damage or theft of any personal mobile device

Academy Provided Mobile Devices (including phones)

- Where the academy provides mobile technologies such as phones, laptops, Digital Cameras and iPads for offsite visits and trips, only these devices should be used
- Where the academy provides a laptop for staff, only this device may be used to conduct academy business outside of the academy.

Passwords and Password Security Password

- **Always use your own** personal passwords
- Make sure you enter your personal passwords each time you log on.
- Do Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of a possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- **Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else**. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished

- **Never tell a child or colleague your password**

Password Security

- Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords private and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security

- Users are provided with an individual network, email, learning and Management Information System log-in username. They are also expected to use a personal password and keep it private

- Students are not permitted to deliberately access on-line materials or files on the school network or local storage devices of their peers, teachers or others

- Staff are aware of their individual responsibilities to protect the security and confidentiality of the academy networks, MIS systems ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

Digital Communication

- Any digital communication (including e.g. email, text and social media) between staff and students or parents/ carers should reflect staff professional integrity and good judgment in line with the Staff Code of practice.

- Email
- The official academy email service may be regarded as safe and secure. Users should be aware that email communication may be monitored.

Staff emails

- Staff should use only the academy email service to communicate with others about school-related business. Users should immediately report to the Headteacher the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Social Media

- Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Staff ***are not*** permitted to access their personal social media accounts

using school equipment at an *time*

- Students are not permitted to access their social media accounts whilst at school

- Staff, IEB, students, parents and carers are aware that their online behaviour should at all times be compatible with UK law

- Not to be online friends with any student (staff should inform the Headteacher of any exceptions

The use of Digital and Video Images

- Photographs and recordings of academy activities and community events are highly valued as a vibrant record of school life and may be used to support and
- document learning or document and promote the school's approach, e.g. on academy notice boards, publicity materials, the academy website and in the press. However, the academy is aware of the risks associated with publishing digital images online.

Parent Consent for Images of Children

Parents are asked to sign a consent form:

1. Whether they consent to the academy taking images of their child.

2. Whether they consent to images of their child being used in external publications (eg the press/ internet).

3. That any images they take of children at the academy will be used appropriately, and in accordance with this policy. Consent forms are held in the school office. A list of students without consent will be kept in the office including LAC students

Images and Video for School Publication

The academy takes steps to protect the identity of all children of whom images are used in academy promotional materials and articles and will only take and use images that are appropriate and not considered to be open to misuse.

1. We do not identify students in online photographic materials (including e.g. in image file names or by including the full names of students in the credits of any published academy video materials/DVDs).

2. If photos of individual children (not group photos) are used on the academy

website or in promotional material the school will obtain parental permission for its long-term, high-profile use.

3. Images of children from the academy will not be used to illustrate controversial subjects. The school ensures that images taken by journalists and other external agencies are subject to the same consents and protective measures as set out above.

The Use of Photography and Recording in the Classroom

Photographs and recordings are useful tools for monitoring children's work and progress, and as such form an essential part of classroom life. Photographic images form a useful part of children's individual Learning Portfolios and provide an opportunity for children to reflect on their own personal growth and development.

The academy takes the following steps to ensure the safe and appropriate use photography and digital recording:

1. Staff discuss the appropriate use of photography with children and supervise any photography undertaken by children in the academy or during off-site activities.
2. Staff ensure all children and adults present are aware of when they are being photographed or filmed, or when a webcam is in use.

3. Digital Cameras are provided for use in each classroom for recording images. The use of staff personal mobile devices for this should not be used in any circumstances.

Policy Monitoring & Review

4. This policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technology, new threats to online safety or incidents that have taken place.

Further Information & Resources

www.thinkuknow.com Information and resources for parents, teachers and young people about staying safe online

https://www.ceop.police.uk for advice, help and to report an incident involving a child's safety online

https://www.iwf.org.uk for reporting criminal online content

KINGSLEY ACADEMY

Nature of incident

□ **Deliberate access**

Did the incident involve material being;
1. created □viewed • printed □shown to others
□transmitted to others • distributed

Could the incident be considered as;
□harassment □grooming □cyberbullying □ breach of AUP

□ **Accidental access**

Did the incident involve material being;
□created □viewed □printed □shown to others
□transmitted to others □distributed

KINGSLEY ACADEMY

Action taken

□ **Staff**

□ incident reported to head teacher/senior manager
□ advice sought from Safeguarding and Social Care
□ referral made to Safeguarding and Social Care
□ incident reported to police
□ incident reported to Internet Watch Foundation
□ incident reported to IT
□ disciplinary action to be taken
□ e-safety policy to be reviewed/amended

Please detail any specific action taken (ie: removal of equipment)

□ **Child/young person**

□ incident reported to head teacher/senior manager
□ advice sought from Safeguarding and Social Care
□ referral made to Safeguarding and Social Care
□ incident reported to police
□ incident reported to social networking site
□ incident reported to IT
□ child's parents informed
□ disciplinary action to be taken
□ child/young person debriefed
□ e-safety policy to be reviewed/amended

Outcome of incident/investigation