

Mobile Phone and Smart Technology Policy

Department: Lifelong learning Key College

Owner: Training & Education Manager/Safeguarding lead

Approval Route: Lifelong Learning Committee

Frequency of Revision: Annual

Version	Date Approved	Reason for Update
1	September 2023	
2	12 March 2024	In response to identified safeguarding need relating to students' own devices.
3	04 March 2025	Updated
4	03 March 2026	Updated

Table of Contents:

Policy Statement
Purpose
Expectations
College provided mobile phones and devices
Staff use of mobile and smart technology
Learners' use of mobile and smart technology
Visitors' use of mobile and smart technology
Monitoring
Responding to breaches
Responsibilities

Appendix

Appendix A - Filtering & Monitoring Settings Procedure

1. Policy statement:

This policy outlines Key College's expectations around the use of mobile and smart devices on our sites. This policy has been developed in cooperation with students, parents/carers and staff taking account of DfE statutory guidance Keeping Children Safe in Education 2025 (KCSIE) and Working Together to Safeguard Children 2023.

2. Purpose

- The purpose of this policy is to safeguard and promote the welfare of all members of the YMCA Derbyshire Key College community when accessing technology, smart devices and social media.
 - YMCA Derbyshire Key College recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm when using social media.
 - As outlined in our safeguarding policy, the Designated Safeguarding Lead (DSL), is recognised as having overall responsibility for online safety.
- The policy applies to all use of social media; the term social media includes, but is not limited to, blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger apps or other online communication services.
- This policy applies to learners, parents/carers and all staff, including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy).
- The Policy outlines the use of all Smart devices and technology.

3. Safe use of mobile and smart technology expectations including watches.

- YMCA Derbyshire Key College recognises that use of mobile and smart technologies is part of everyday life for many learners, staff and parents/carers.
- Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of the YMCA Derbyshire Key College community are advised to:
 - Take steps to protect their mobile phones or personal devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
 - Use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on their phones or devices.
- Personal mobile phones and devices are not permitted to be used in specific areas on site, such as toilets & classrooms (without tutor and centre manager permission).
- Ensure that SMART glasses and all watches are removed and not permitted during formative and summative assessments and accessed during sessions.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with in line with our Behaviour Management and Antibullying policy, Conduct and Professional Boundaries procedure and Safeguarding policies.

- All members of the YMCA Derbyshire Key College community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our Behaviour Management and Antbullying policy, Conduct and Professional Boundaries procedure and Safeguarding policies.
- Photographs will not be taken on site using mobile phones or personal devices except on devices designated as work-related technology. Photographs will only be taken where prior consent has been agreed with the learner and/or parental/guardian permission has been granted depending on age and capacity.
- External or personal devices owned by either a student, staff member, volunteer or visitor will not be granted access to Wi-Fi unless through a guest network.
- Any personal external devices including, but not limited to, USB sticks, mobile phones, tablets, laptops etc, are not permitted to be used or accessed, or charged, using YMCA Derbyshire devices, unless agreed by a Senior Leader or Manager.

4. Mobile phones and devices provided by YMCA Derbyshire Key College:

- Members of staff will be issued with a work phone number in addition to their work email address, where contact with learners or parents/carers is required. Internal work phones or the above stated devices will be the only devices used to contact students.
- Staff providing formal remote learning will do so using equipment provided by YMCA Derbyshire Key College in accordance with our Computer policy and Remote Learning policy.
- YMCA Derbyshire Key College mobile phones and devices will be suitably protected via a passcode/password/PIN and must only be accessed or used by members of staff.
- YMCA Derbyshire Key College mobile phones and devices will always be used in accordance with this policy and other relevant policies.
- Where staff are using mobile phones and/or devices provided by YMCA Derbyshire Key College they will be informed prior to use via our Computer policy that activity may be monitored for safeguarding reasons and to ensure policy compliance.

5. Staff use of mobile and smart technology

Members of staff will ensure that use of any mobile and smart technology, including personal phones and mobile devices, will take place in accordance with the law, as well as relevant YMCA Derbyshire Key College policies and procedures, including Confidentiality, Safeguarding, Data Protection, Behaviour management and Antbullying policies, Code of Conduct polices, the Maintaining Professional Boundaries procedure and all policies relating to the use of computers and information technology (IT).

- Staff will be advised to:
 - Keep mobile phones and personal devices in a safe and secure place during lesson time.
 - Keep personal mobile phones and devices switched off or set 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 centre manager/head of service/director, such as in emergency circumstances.
- Only use personal mobile devices in staff-only areas such as staff offices and break rooms or off site.
- Ensure that any content bought onto site via personal mobile phones and devices is compatible with their professional role and our behaviour expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.
 - Any pre-existing relationships or circumstance which could compromise ability to comply with this, must be declared and will be discussed with the DSL and the relevant centre manager.
- Staff will only use equipment provided by YMCA Derbyshire Key College (and not personal devices):
 - to take photos or videos of learners in line with our image use policy;
 - to work directly with learners during lessons/educational activities; and
 - to communicate with parents/carers.
- Where remote learning activities take place, staff will use equipment provided by YMCA Derbyshire Key College. If this is not available, staff will only use personal devices with prior approval from the centre manager following a formal risk assessment. Staff will follow clear guidance outlined in the Remote learning policy.
- If a member of staff breaches our policy, action will be taken in line with our staff Behaviour Management and Antibullying policy and Code of Conduct policy and Maintaining Professional Boundaries document.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or to have committed a criminal offence using a personal device or mobile phone, the police will be contacted, and the LADO (Local Authority Designated Officer) will be informed in line with our policy on handling allegations, and follow other appropriate channels of reporting.

6. Learner's use of mobile and smart technology

- Learners will be educated regarding the safe and appropriate use of mobile and smart technology, including mobile phones and personal devices, and will be made aware of behaviour expectations and consequences for policy breaches.
- Safe and appropriate use of mobile and smart technology will be taught to learners as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our Safeguarding policy.
- Learners will not be allowed to take photos or videos of other Key College learners, staff members or facilities including classroom and communal spaces at any Key College centre.
- Classroom expectations around the use of mobile and smart devices will be displayed in all classrooms and be consistent across all centres.
- Learners using mobile phones and/or personal devices will follow these guidelines:
 - Mobile phones or personal devices will not be used by learners during lessons or formal educational time.

- Students will not be allowed to listen to music through their mobile phone devices. Where a situation enables a student one-to-one support or self/independent study outside of regular sessions then this may be granted with manager's and tutor's agreement.
- Mobile phones or personal devices can be used by learners during break or free time, but any use must be in accordance with our Anti-bullying and Behaviour policy. If learners breach our policies, this may be revoked.
- Students' mobile phones or personal devices used by students during break/free time will not be permitted to connect to YMCA Derbyshire Wi-Fi.
- Laptops or PCs issued to learners for teaching and learning purposes will only be those devices registered as YMCA Derbyshire Key College devices.
- YMCA Derbyshire Key College expects personal devices and mobile phones to be kept safe and secure when on site. This means phones:
 - should be on silent or switched off; and
 - remain away from desks and tables and kept in pockets or bags during the lesson.
- If a learner needs to contact their parents or carers whilst on site, they will be allowed to use a YMCA Derbyshire Key College phone.
 - Parents are advised to contact their child via the YMCA Derbyshire Key College office; exceptions may be permitted on a case-by-case basis, as approved by the centre manager.
- If a learner requires use of their personal device in lessons in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with the centre manager and tutor prior to use being permitted.
 - Any arrangements regarding access to personal devices in exceptional circumstances will be documented and recorded by YMCA Derbyshire Key College.
 - Any specific agreements and expectations, including sanctions for misuse, will be provided in writing and agreed by the learner and their parents/carers before use is permitted.
- Where learners' mobile phones or personal devices are used when learning at home, this will be in accordance with our Remote Learning policy.
- Mobile phones and personal devices must not be taken into examinations. Learners found in possession of a mobile phone or personal device which facilitates communication or access to the internet during an exam will be withdrawn from the exam. Where a breach has occurred, the examining body will be contacted.
- Any concerns regarding learners' use of mobile technology or policy breaches will be dealt with in accordance with our existing policies, including Safeguarding, Remote Learning and Behaviour Management and Antbullying policies.
 - Searches of mobile phone or personal devices will not be carried out by staff members. If it is believed that a criminal offence has occurred YMCA Derbyshire Key College will contact the parent/guardian and the police where appropriate.
 - Appropriate pastoral/welfare support and/or sanctions will be implemented in line with our Behaviour Management and Antbullying policy and Safeguarding policy.
 - Concerns regarding policy breaches by learners will be shared with parents/carers as appropriate.

- Where there is a concern that a child is at risk of harm, we will respond in line with our Safeguarding policy.
- If there is suspicion that material on a learner's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

7. Visitors' use of mobile and smart technology

- Parents/carers and visitors, including volunteers and contractors, are expected to ensure that:
 - Personal devices are not to be used in communal areas of YMCA Derbyshire Key College; this includes our classrooms, offices, and break rooms for students and staff. Personal calls may be made in reception areas of each building.
 - Personal phone calls are made off site.
 - No photos are taken using any device.
 - Personal devices are to be switched off on arrival onto YMCA Derbyshire Key College premises.
- Appropriate signage and information is displayed in communal areas to inform visitors of our expectations for safe and appropriate use of personal devices and mobile phones.
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use mobile and smart technology in accordance with this policy and other associated policies, including the Safeguarding policy.
- If visitors require access to mobile and smart technology, for example when working with learners as part of a multi-agency activity, this will be discussed with the centre manager prior to use being permitted.
 - Any arrangements regarding agreed visitor access to mobile/smart technology will be documented and recorded by YMCA Derbyshire Key College in line with the External speaker policy. This may include undertaking appropriate risk assessments if necessary.
- Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL at YMCA Derbyshire of any breaches of our policy.

8. Monitoring of digital equipment:

- All devices that connect to YMCA Derbyshire Key College's network will be monitored regarding the content that those devices access. Activity on the student laptops will also be key logged with triggered screenshots, and the potential for the Tutor to remote view the screens during lessons.
- This is through the
 - Smoothwall appliance on the edge of each network and the Smoothwall Cloud Filter client on every laptop and PC in Key College for web content monitoring and alerts. Smoothwall Cloud Filter Client is configured to filter and block categories that are illegal, harmful or inappropriate. When attempts to access content or carry out Web searches constitute a potential safeguarding concern, a safeguarding alert e-mail is sent to the

Designated Safeguarding Lead, the Manager of each Key College campus and the Quality & Compliance Assistant.

- Smoothwall Monitor client on each student laptop for keylogging and input monitoring. Smoothwall Monitor sends keylogging data to an external safeguarding centre and captures a screenshot when triggered by a keyword. Results are monitored by Smoothwall Limited and if their team consider there to be immediate risk, they will telephone the Designated Safeguarding Lead or the manager of the Key College campus.
- Senso Cloud Classroom Management Software on each student laptop to enable the Tutor's remote viewing of students' screens during sessions for direct physical monitoring.
- This filtration and monitoring protects the user of the device from accessing harmful content. The clients on the device reads Domain Name System (DNS) requests made from the machine and sends these to a Cloud Filter service for analysis against a category list of webpages held by Smoothwall Limited. The machine is protected regardless of which network it is connected to, or where the machine is.
- External devices on the guest Wi-Fi have the same filtering as Key College devices because all traffic passes at the Key College campuses passes through the Smoothwall appliance as the edge router.
- The user and machine are identifiable from username and host name in the logs and e-mail alerts.
- Please see the Filtering & Monitoring Settings Procedure, attached as Appendix A, as to which actions are applied to which category of page or which observed event.

9. Responding to policy breaches

All members of the community are informed of the need to report policy breaches or concerns in line with existing YMCA Derbyshire policies and procedures. This includes the Behaviour Management and Antibullying policy, Safeguarding policy, Code of Conduct policy and Maintaining Professional Boundaries document.

- After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
- We require staff, parents/carers and learners to work in partnership with us to resolve issues.
- All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.
- Learners, parents and staff will be informed of our Complaints policy and procedure.

10. Artificial Intelligence

-This policy links directly to YMCA Derbyshire's AI policy and the assessment, quality assurance and malpractice policy in regards to the use and application of artificial intelligence on YMCA Derbyshire Key College.

Responsibilities:

- All Key College staff
- Volunteers
- Students
- Visitors
- YMCA Derbyshire safeguarding team

Appendix A - Filtering & Monitoring Settings Procedure

Smoothwall Cloud Filter has been configured to block for the following categories which are harmful, illegal or inappropriate:

- Child abuse (keywords provided by the IWF)
- Terrorism (pages provided by the OSCT at the Home Office)
- Criminal activity (for example, instructions on lock picking or committing fraud)
- Drugs (sale, manufacture or promotion of recreational and prescription drugs)
- Cannabis (pages about the use or cultivation of cannabis)
- Hacking (pages about hacking)
- Intolerance (pages that Smoothwall Ltd deems to promote intolerance)
- Self-harm (pages about suicide, self-harm and eating disorders)
- Violence (pages about violence)
- Weapons (pages discussing weapons)
- Military (military weapons including in military history)
- Hunting (hunting and shooting weapons)
- Fireworks (page for the purchase of fireworks)
- Pornography (textual or visual sexual content)
- Sexual (Content based primarily on sexuality which may be unsuitable for a younger audience.)
- Nudity (Sites about naturism or which contain nudity)
- Swimwear (pictures of revealing attire)
- Unmoderated image hosting
- File sharing
- Peer-to-Peer
- Gambling (betting, bookmakers and casinos)
- Academic dishonesty (plagiarism aids)
- Alcohol and tobacco (sites about the use or sale of alcohol or tobacco)
- Gore (gory content)
- Vulgar search terms
- VPNs and proxies (sites that bypass filtering or geographic restrictions)
- Messaging and conferencing (instant messaging or video calls)
- Social networking
- Omegle
- Piracy

Student users are also blocked by Smoothwall Cloud Filter from

- Video streaming, music, cartoons and film

Exceptions are in place for Microsoft 365 and individual exceptions for those social networks, video calling and streaming services used in teaching and learning, and for local sexual health services.

Following an initial review at deployment of the sensitivity settings by the Training & Education Managers and the Quality & Compliance Assistant, Smoothwall Monitor has been configured to alert the Designated Safeguarding Lead, the manager of each Key College campus and the Quality & Compliance Assistant when the following are observed:

- a mildly offensive comment is typed about another person
- a sexual reference or innuendo is typed
- a strongly offensive word is typed
- a user discloses their full address or bank details inappropriately
- a user researches weapons
- a user communicates with an adult and this may progress to grooming
- a user types sympathies for those who have committed acts of terrorism
- a user expresses suicidal feelings or conducts detailed research into helplines not in an identifiable research context
- any situations where Smoothwall Limited's team spot something concerning which they feel Key College should be alerted to.

We will conduct an annual review of our online filtering and monitoring software to ensure that it remains fit for purpose.