OFG Education

MOBILE & SMART DEVICE POLICY

Castle Garden School

Designated Safeguarding Lead:
Gillian Rolfe
Safeguarding Governor:
Lorna Davies-Bailey

MOBILE & SMART DEVICE POLICY

CONTENTS **PAGE**

1.0 POLICY STATEMENT..... 3
2.0 SCOPE..... 3
3.0 POLICY FRAMEWORK..... 4
4.0 SAFE USE OF MOBILE AND SMART DEVICES EXPECTATIONS 5
5.0 STUDENTS' USE OF MOBILE AND SMART DEVICES 6
6.0 SEARCHES, SCREENING AND CONFISCATION..... 7
7.0 TEAM MEMBERS' USE OF MOBILE AND SMART DEVICES 8
8.0 MOBILE PHONES AND DEVICES PROVIDED BY THE SCHOOL/COLLEGE 10
9.0 VISITORS' USE OF MOBILE AND SMART DEVICES 11
10.0 RESPONDING TO POLICY BREACHES 12
11.0 POLICY MONITORING AND REVIEW..... 13

Terminology

Please note that the terms:

- "**Our teams**" and" "team members" include everyone working in Outcomes First Group's settings and services in a paid or unpaid capacity, including employees, consultants, agency staff, trainees and contractors (and volunteers in our Blenheim Schools).

- "**Parents and carers**" refer to the person or people with legal parental responsibility for the child/young person
- "**Students**" refers to all children and young people being educated and supported at the setting or service
- "**Personal device**" means any privately owned mobile phone, tablet, laptop, smart watch, wearable device or other equipment capable of communication, internet access, audio or image recording, or receiving notifications.

- "**School/college-provided device**" means a device owned, leased or expressly authorised by Outcomes First Group or the education setting for educational, operational, communication or safeguarding purposes.

1.0 POLICY STATEMENT

The safety of our students is our highest priority. The use of mobile and smart devices is part of everyday life, providing many possibilities and opportunities for learning whilst also bringing significant risks.

DfE has introduced Mobile phones in schools statutory guidance, which states that **schools should operate as mobile-phone-free environments by default**, anything other than this should be by exception only. The Proprietor and the Headteacher must have regard to this statutory guidance. Scottish Guidance and Welsh Guidance also aim to create phone-free learning environments. Any use of mobile phones in schools will be by exception and will need to be approved by the Headteacher/ Principal, in agreement with the Regional Director/ Operations Director.

The purpose of this policy is to safeguard and promote the welfare of all members of the school/college community regarding the use of mobile devices and smart devices in the setting's environment and is fully endorsed by the school's/college's governing body.

This policy seeks to minimise disruption, support positive behaviour, safeguard our students, and create a safe and focused learning environment in which students can fully engage in education while continuing to develop the knowledge and skills needed to use technology responsibly and safely

Post 16 and Further Education provisions have the opportunity to be more flexible with students who are over 16 years of age, who may be able to have access to their mobile phones at certain times and locations. Such flexibility will be carefully managed, risk assessed and proportionate, balancing the development of personal responsibility with the need to maintain a safe and focused learning environment.

Access to mobile phones for post 16 students will be limited to the documented purposes and locations, be risk assessed, and must not undermine the settings phone-free environment therefore should not be visible to younger students.

This policy and any setting-specific arrangements will be communicated to students, parents/carers, team members and visitors. Expectations will be reinforced through induction, curriculum teaching, signage, reminders and consistent responses to breaches.

2.0 SCOPE

This policy applies to all education settings and to students, visitors, team members, and other individuals who provide services on behalf of the school/college. It applies to all mobile devices and smart devices on site, including but not limited to, mobile phones and personal devices, such as tablets, e-readers, games consoles and wearable technology, such as smart watches, fitness trackers, and Meta glasses which facilitate communication or have the capability to record sound or images.

This policy also covers educational visits, off-site activities, work experience, alternative provision, transport or journeys organised by the setting, and remote or virtual education where relevant.

3.0 POLICY FRAMEWORK

This policy has also been developed in line with DfE's guidance:

- Keeping children safe in education (KCSiE)
- Working Together to Safeguard Children;
- Searching, Screening and Confiscation
- Teaching Online Safety in Schools
- How to respond to an incident of nude/ semi-nude images being shared
- Behaviour in Schools

and the:

- Education Act 1996, section 550C, as inserted by the 2026 legislation;
- Equality Act 2010
- Data Protection Act 2018 and UK GDPR;

We recognise that legislation and guidance around this important matter are continuing to develop at pace. This policy will be reviewed and updated as further national requirements and guidance are published.

This policy should read alongside other school and Group policies, including:

- AI Policy and AI Acceptable Use Policy
- Anti-bullying Policy
- Relational & Inclusive Behaviour Policy
- Child-on-child Abuse Policy
- Code of Conduct & Ethics (CoCE)
- Complaints Policy
- Cyber Security Policy
- Data Protection Policy
- Information Security Policy

- Managing Allegations Against an Employee Policy
- Mobile Device Policy (IT Policy)
- Relationships, Sex and Health Education (RSHE) Policy
- Safeguarding Policy
- Searching, Screening and Confiscation Policy
- Serious Incident Notification Policy
- Staying Safe Online
- Qualification policies
- Use of Images & Consent Policy
- Visitors and Visiting Speakers Policy (Blenheim Schools)
- Web Filtering & Monitoring Policy
- Whistleblowing Policy

4.0 SAFE USE OF MOBILE AND SMART DEVICES EXPECTATIONS

4.1 We recognise that use of mobile and smart devices is part of everyday life for students, team members and parents and carers. As part of the introduction and induction to the school/college the Headteacher/ Principal will clearly explain this policy to the student and their parents/carers, and how it has been developed in best interests of students to create a safe and positive learning environment.

4.2 All members of the school/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 or safeguarding policies. (Please see 7.0 Team Members' Use of Mobile and Smart devices).

4.3 The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school/college community. Any breaches will be dealt with in line with the anti-bullying, behaviour and safeguarding policies, and where appropriate, the *Code of Conduct & Ethics*.

All members of the school/college community are advised to use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on their phones or devices.

4.4 Governors, proprietors and school leaders, working with the IT Team, will ensure appropriate filtering and monitoring systems are in place and reviewed in line with KCSIE and the *Web Filtering & Monitoring Policy*.

5.0 STUDENTS' USE OF MOBILE AND SMART DEVICES

5.1 Students must not access or use mobile phones or smart devices with similar functionality at any point during the school/college day, including lessons, transitions, breaktimes and lunchtime, unless a documented exception applies. Technology required for learning will be provided by the school.

5.2 Personal electronic devices, including phones, smart watches and tablets, brought onto site by students must be handed in at the school/college reception. They will be put into a pouch or box that blocks signals. Students are asked to switch the device off or put it into aeroplane mode before it is placed in the pouch or box. The devices will be stored safely in a locked cupboard **until the end of the school/college day** when students can collect them from the school/college office.

Exceptional Circumstances - If a student requires access to a personal device in exceptional circumstances due to reasonable adjustments, SEND, disability, medical conditions, and individual circumstances such as young carers or other safeguarding-related communication needs, this will be discussed with the Headteacher/Principal prior to use being permitted, who will seek advice from the Clinical Team on this matter. Any arrangements regarding access to personal devices in exceptional circumstances will be documented and recorded by the school/college and **must be approved by the Regional Director/ Operations Director**. Specific agreements and expectations (including sanctions for misuse) will be clearly communicated, provided in writing and agreed by the student and/or their parents/carers before use is permitted.

Students with an agreed exception may use the device **only for the agreed purpose, at agreed times and locations, and under agreed supervision/monitoring arrangements where necessary**.

Students aged 16 and over may, where appropriate, be given greater flexibility in the use of personal mobile devices, for example having access to their mobile device during off-site visits or while travelling. Any such arrangements will be carefully considered, proportionate and based on an individual or activity-specific risk assessment, balancing the development of personal responsibility and independence with the need to maintain a safe, calm and purposeful learning environment. Any permitted use of personal devices will be restricted to clearly defined times, locations and purposes, which will be clearly communicated to students and team members. **If the provision intends to allow such flexibilities, they must set out their bespoke approach as an attachment to this policy and have it signed off by the Regional Director/ Operations Director.**

5.3 If parents/carers need to contact the student during school/college hours, they should contact the school/college office on the telephone number on the school's/college's website. If a student needs to contact their parents/carers whilst on site, they will be allowed to use a school/college phone.

5.4 Students will be educated regarding the safe and appropriate use of mobile and smart devices, including the risks and benefits of their use and the reasons for the school/college's mobile-phone-free environment. They will be made aware of behaviour expectations and consequences for policy breaches. Safe and appropriate use of mobile and smart devices will be taught as part of an embedded and progressive safeguarding education approach, using ageappropriate sites and resources.

5.5 Mobile phones and personal devices must not be taken into examinations or tests. Students found in possession of a mobile phone or personal device which facilitates communication or internet access during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations. Please see the *Qualification policies* for further information.

5.6 Where a student's mobile phone and/or personal devices are used when learning at home, this will be in accordance with the Group's *Mobile Device Policy* and should be supervised by the parent or carer.

5.7 Any concerns regarding a student's use of mobile technology or policy breaches will be dealt with in accordance with our existing Behaviour and related policies.

5.8 This policy applies when students take part in off-site activities and trips during the school/college day. The student's personal device should be kept at the school/college and collected at the end of the school/college day as usual (please see 5.2 regarding students over 16). If a student may require a mobile phone for safety reasons, the school/college will provide a basic mobile phone for the student.

On occasions where a student is travelling directly to an external provider's site and not coming into school/college first, they must comply with the provider's arrangements regarding personal devices.

Before an educational visit, work-experience placement, alternative-provision placement or other off-site activity, the setting must identify and communicate the applicable device arrangements. Any exception must be recorded in the activity or individual risk assessment and shared with relevant team members and the provider.

6.0 SEARCHES, SCREENING AND CONFISCATION

6.1 Any screening, searching and confiscation that is required in the school/college will be carried out in accordance with the DFE's Searching, Screening and Confiscation guidance and the Group's *Searching, Screening and Confiscation Policy*.

6.2 Schools/colleges may use screening devices to check that students do not have devices or other prohibited items on them. Any such arrangements should be proportionate and risk based. The local police should be consulted before the introduction of screening technology and must be approved by the Regional Director/ Operations Director and Headteacher/Principal prior to the introduction. Students and parents/carers/those with parental responsibility must also be informed, before the technology is introduced, with an explanation of what it will involve and why it is being introduced.

6.3 Only the Headteacher/Principal, or an appropriately authorised team member may carry out a search where the relevant legal and policy requirements are met. Searches must be necessary, proportionate and sensitive to the student's age, communication needs, disability, SEND, sensory profile and previous experiences.

6.4 A confiscated electronic device must be stored securely. Its data or files must not be accessed solely because the device has been confiscated. Any examination of a device or its data must be lawful, necessary, proportionate and undertaken only by an appropriately authorised person in accordance with the OFG Searching, Screening and Confiscation Policy.

Where a device may contain evidence of an offence or material giving rise to a safeguarding concern, the device must be secured and the Designated Safeguarding Lead (DSL) informed immediately. **Team members must not unnecessarily view, copy, print, forward, share, store, save, alter or delete the material.**

Where a concern involves nude or semi-nude images or videos of a child or young person, team members must follow the *Safeguarding Policy* and UKCIS guidance. Such imagery must not be viewed unless this is unavoidable and expressly permitted under that guidance.

The DSL will determine whether children's social care, the police, parents or carers, the placing authority (where relevant) or another agency should be informed. **Where there is an immediate risk of serious harm or an emergency, the police must be contacted without delay.**

The Director of Safeguarding/ Safeguarding Adviser must be informed by emailing safeguarding@ofgl.co.uk in line with the Safeguarding Policy.

7.0 TEAM MEMBERS' USE OF MOBILE AND SMART DEVICES

7.1 During school/college hours, team members will only use mobile and smart devices provided by the school/college that have been purchased via the IT Service Desk. The school/college must ensure there is a sufficient supply of company mobile devices available for team members to use on site and take with them on school/college visits and journeys off site.

Team members' personal devices, including mobile phones and smart watches, must be switched off or placed in aeroplane mode and stored securely while team members are working with or in areas accessible to students, unless an authorised exception applies. If team members need to provide daytime contact details for emergency purposes, they should provide the school/college office number.

Team members may access personal devices during authorised breaks only in designated staff-only areas, provided this does not compromise supervision, safeguarding, professional boundaries or operational responsibilities.

Where an authorised personal device is required for multi-factor authentication, password recovery or another approved security process, it may be used briefly in a designated staff-only area in accordance with the Group's information security and BYOD requirements. The device must not be used in the presence of students and must be securely stored immediately afterwards.

Team members that need to use their personal mobile phone to reset their Group login password or access Outcomes First Group's IT systems that require twofactor authentication, can do so in a room not accessed by students e.g. the school/college office or staffroom. Their personal mobile phone should only be used for this purpose and must then be turned off or put on aeroplane mode and locked away after use.

Exceptional Circumstances – A team member may be permitted to retain or use a personal device where this is required as a reasonable adjustment, for an agreed medical or accessibility purpose, or in another exceptional circumstance authorised by the Headteacher/Principal and the Regional Director/ Operations Director. Any arrangements regarding access to personal devices in exceptional circumstances must be documented and recorded by the school/college. Team members with an agreed exception may use the device only for the agreed purpose, times and locations.

7.2 In an emergency, a team member may use the most immediately available means of communication to protect life or prevent serious harm. The use must be reported and recorded as soon as practicable.

7.3 Team members will use mobile and smart devices in accordance with the law, DFE guidance and the relevant Group and school/college policies.

7.4 Team members are advised to: • Ensure that any content brought onto site via personal mobile phones and devices is compatible with their professional role and our behaviour expectations.

- Be aware that they are not permitted to use their own personal phones or devices for contacting learners or parents and carers at any time. Any preexisting relationships or circumstance which could compromise a team member's ability to comply with this will be discussed with the DSL and the Headteacher/Principal.

- If a team member 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 Local Authority Designated Officer or equivalent will be informed in line with the *Managing Allegations Against an Employee Policy*.

  This matter must be reported to the DSL and recorded, Human Resources peopleadvice@ofgl.co.uk and Safeguarding (safeguarding@ofgl.co.uk) should be informed, as appropriate.

- Team members must not use personal or school/college provided devices to create, modify, generate, share, or store AI-generated, digitally altered, or synthetic images, audio, or video of students, colleagues, parents, carers or visitors unless there is a legitimate educational or business purpose, appropriate authorisation and compliance with the *AI Acceptable Use Policy, Data Protection Policy, and Use of Images & Consent Policy.* Content created for humour, parody, or entertainment that could reasonably cause offence, embarrassment, distress or reputational harm is prohibited.

  If a team member breaches this policy, action will be taken in line with the *Code of Conduct & Ethics* and *Managing Allegations Against An Employee Policy*.

8.0 MOBILE PHONES AND DEVICES PROVIDED BY THE SCHOOL/COLLEGE

8.1 Devices and equipment required for teaching, learning, contacting parents/carers/those with parental responsibility, for safety reasons, will be provided by the school/college and must be used in accordance with the Group's *Mobile Device Policy* and other relevant policies.

8.2 Team members providing formal remote learning will do so using school/college provided equipment in accordance with the Group's *Mobile Device Policy* and *Code of Conduct & Ethics Policy*.

8.3 School/college mobile phones and devices will be suitably protected via a passcode/password/PIN and must only be accessed or used by team members and/or students with prior permission.

8.4 Where team members and/or students are using school/college provided mobile phones and/or devices, they will be informed prior to use via the *Mobile Device Policy* and user agreements that activity may be monitored for safeguarding reasons and to ensure policy compliance.

8.5 Team members will only use equipment provided by the school/college (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.
- to communicate with parents/carers.

School/college-provided devices must be configured, managed and used in accordance with OFG information-security, acceptable-use, data-protection and mobile-device requirements. Users must not disable security controls, install unauthorised applications, use personal accounts to store OFG information, or permit unauthorised access.

Loss, theft, damage, suspected compromise or unauthorised access must be reported immediately through the applicable IT, data-protection and safeguarding procedures.

Images, recordings and personal information relating to students must be captured, stored, accessed, shared and deleted only for authorised purposes and in accordance with the *Use of Images and Consent Policy*, Data Protection Policy and retention requirements.

9.0 VISITORS' USE OF MOBILE AND SMART DEVICES

- Parents/carers and visitors, including contractors and volunteers (Blenheim schools), are asked not to use their mobile phones or smart devices whilst on the school/college premises. They should be stored securely when not being used and locked with appropriate security settings (e.g. passcode/passwords/pin numbers). They should be switched off, or put on aeroplane mode, when at the school/college.
- Clear signage and information are displayed in reception to inform visitors of our expectations for safe and appropriate use of personal devices and mobile phones. All visitors will be asked to agree to comply with these arrangements when they sign in at the school/college reception.
- **Under no circumstances should a visitor allow a student to use their mobile device. All devices must be passcode\password\PIN protected and locked if left unattended.**
- Visitors, including contractors and volunteers (Blenheim Schools), who are on site for regular or extended periods of time are expected to use mobile and

smart devices in accordance with the *Mobile Device Policy* and other associated policies, including the Safeguarding Policy.

- If visitors require access to mobile and smart devices, for example when working with students as part of multi-agency activity, this will be discussed with the Headteacher/Principal prior to use being permitted. Any arrangements regarding agreed visitor access to mobile/smart devices will be documented and recorded by the school/college. This may include undertaking appropriate risk assessments if necessary.
- Team members are expected to challenge visitors if they have concerns about their use of mobile and smart devices and inform the DSL or Headteacher/ Principal of any breaches of the policy.

10.0 RESPONDING TO POLICY BREACHES

- Responses must be proportionate to the nature, seriousness and context of the incident and must take account of the student's age, needs, communication, disability, SEND and individual circumstances.
- Routine breaches will be managed in accordance with the *Behaviour Policy* and any agreed individual plan. Responses should be consistent, educational and proportionate.
- **Safeguarding concerns** must be reported immediately to the DSL or deputy and recorded on the setting's electronic recording system on the same day. The DSL must assess the concern and make any necessary referral without delay. An internal reporting timescale must never delay contact with children's social care, the police or another safeguarding agency.
- **Concerns about a team member, contractor or volunteer** must be managed under the *Managing Allegations Against an Employee Policy* and the *Low-level Concerns Policy* arrangements, as applicable.
- **Suspected criminal conduct or potential evidence of an offence** must be managed in consultation with the DSL. Relevant evidence must be preserved and the school or college must avoid action that could interfere with a police investigation.
- **Data-protection or information-security incidents** must be reported immediately through the applicable OFG data-protection, cyber-security and IT incident procedures in line with the policies.
- Where there is an immediate risk of serious harm or an emergency, the police or emergency services must be contacted without delay.
- Parents or carers will normally be informed of concerns involving their child unless doing so would place the student or another person at increased risk, prejudice an investigation, or be contrary to advice from a statutory agency.
- Following a significant incident, leaders will review the response, identify lessons and make any necessary changes to risk assessments, individual plans, staff guidance, curriculum provision or local arrangements.
- All team members are informed of the need to report policy breaches or concerns in line with existing policies and procedures as part of their induction and training.

- Should any mobile/smart device related incidents occur, team members must prioritise the student's immediate safety. They must remain professional and adhere to all safeguarding and confidentiality procedures.
- The DSL or deputy must be informed immediately. This must be done verbally and then followed up **on the same day** and documented on the school's/college's electronic recording system and the Director of Safeguarding/Safeguarding Adviser notified via email: safeguarding@ofgl.co.uk
- On receipt of the information, the DSL must consider all information and then, in cases of serious concern, report this within **one working day** to the host authority, placing authority, Regional Director/ Operations Director, and where relevant, the Local Authority Designated Officer or local equivalent.
- **If there is suspicion that a student's personal device or mobile phone contains or may provide evidence relating to a criminal offence, the device must be confiscated and handed over to the police for further investigation. (Please also see 4.3)**
- After any investigations are completed, leadership team members will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
- Team members, parents/carers/those with parental responsibility and students are required 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.
- Students, parents/carers and team members will be informed of our complaints procedure and team members will be made aware of the ***Whistleblowing Policy***.
- If the school/college is unsure how to proceed with an incident or concern, the DSL/Deputy or Headteacher/Principal will seek advice from the Regional Director/ Operations Director.

11.0 POLICY MONITORING AND REVIEW

- Technology evolves and changes rapidly. This policy will be reviewed at least annually. The policy will be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure. Where necessary, updates will be made during the year.

- We will regularly monitor internet use taking place via our provided devices and systems and evaluate online safety mechanisms to ensure that this policy is consistently applied. (Please see the ***Web Filtering Policy***) Any issues identified will be incorporated into our action planning.



OFG
Education