CITY OF ROCHESTER SCHOOL MOBILE AND SMART TECHNOLOGY POLICY

This policy, which applies to the whole school, and upon request a copy (which can be made available in large print or other accessible format if required) may be obtained from the School Office. This policy is also publicly available on the school website

Monitoring and Review:

This policy is subject to continuous monitoring, refinement and audit by the Headteacher. The Headteacher will undertake a full annual review of this policy and procedures, inclusive of its implementation and the efficiency with which the related duties have been discharged. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay.

Signed:

Date Reviewed: September 2023 Date of Next Review: September 2024 Version No. 3

Alicja Emmett Headteacher

This policy will be reviewed no later than September 2023, or earlier if changes in legislation, regulatory requirements or best practice guidelines so require.

1. Policy aims and scope

- This policy has been written by Michelle Homer, involving staff, pupils and parents/carers, building on Kent County Councils Education Safeguarding Service's mobile and smart technology policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance '<u>Keeping Children Safe in Education'2023</u>, '<u>Working Together to Safeguard Children</u>'2018, '<u>Behaviour in Schools Advice for headteachers and school staff'2022</u>, '<u>Searching, screening and confiscation at school'</u> 2022 and the local <u>Kent Safeguarding Children Multi-agency Partnership</u> (KSCMP) procedures.
- The purpose of this policy is to safeguard and promote the welfare of all members of our community when using mobile devices and smart technology.
 - City of Rochester School recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm when using mobile and smart technology.
 - As outlined in our Child Protection Policy, the Designated Safeguarding Lead (DSL), Kelly Lovell, Assistant Head, is recognised as having overall responsibility for online safety.
- This policy applies to all access to and use of all mobile and smart technology on site; this includes but is
 not limited to mobile/smart phones and personal devices such as tablets, e-readers, games consoles and
 wearable technology, such as smart watches and fitness trackers, which facilitate communication or have
 the capability to record sound and/or images.
- This policy applies to pupils, parents/carers and all staff, including the trustees, 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).

Page 1 of 6

2. Links with other policies

- This policy links with several other policies, practices and action plans, including but not limited to:
 - Anti-bullying policy
 - Acceptable Use Policies (AUP)
 - Positive behaviour policy
 - Child protection policy
 - Staff code of conduct/staff behaviour policy
 - Confidentiality policy
 - Curriculum policies, such as: Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
 - Data security
 - o Online Safety
 - Social media policy

3. Safe use of mobile and smart technology expectations

- City of Rochester school recognises that use of mobile and smart technologies is part of everyday life for many pupils, staff and parents/carers.
- Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of our community are advised to:
 - take steps to protect their personal mobile phones or other smart 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 personal phones or devices.
- Mobile devices and other forms of smart technology are not permitted to be used in specific areas on site; this includes in classrooms and in meetings.
- The sending of abusive or inappropriate messages or content, including via personal mobile devices and/or smart technology is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying, behaviour and child protection policies.
- All members of the City of Rochester School community are advised to ensure that their personal mobile and smart technology devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our behaviour or child protection policies.

4. City of Rochester School provided mobile phones and devices

- Staff providing formal remote/online learning will do so using City of Rochester school provided equipment in accordance with our remote learning policy.
- School devices will be suitably protected via a password and must only be accessed or used by members of staff and/or pupils.
- City of Rochester School mobile phones or devices will be suitably protected via a password and must only be accessed or used by members of staff and/or pupils.
- City of Rochester school mobile phones and/or devices will always be used in accordance with our staff code of conduct/behaviour policy, acceptable use of technology policy and other relevant policies.
- Where staff and pupils are using school provided mobile phones and devices, they will be informed prior to use via our Acceptable Use Policy (AUP) that activity may be monitored for safeguarding reasons and to ensure policy compliance.

Page 2 of 6

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 wearable technology and other mobile/smart devices, will take place in accordance with the law, as well as relevant school policy and procedures, including confidentiality, child protection, data security staff behaviour/code of conduct and Acceptable Use Policies.
- Staff will be advised to:
 - Keep mobile and smart technology devices in a safe and secure place during lesson time.
 - Keep personal mobile phones and devices switched off or set to 'silent' or 'do not disturb' modes during lesson times.
 - Ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
 - Not use personal mobile or smart technology during teaching periods unless written permission has been given by the headteacher, such as in emergency circumstances.
 - Ensure that any content bought onto site via personal mobile and smart technology devices is compatible with their professional role and our behaviour expectations.
- Members of staff are not permitted to use their own personal mobile and smart technology devices for contacting pupils or parents and carers.
 - Any pre-existing relationships or circumstance, which could compromise staff's ability to comply with this, will be discussed with the DSL and headteacher.
- Staff will only use school provided equipment (not personal devices):
 - \circ to take photos or videos of pupils in line with our image use policy.
 - to work directly with pupils during lessons/educational activities.
 - to communicate with parents/carers.
- Where remote learning activities take place, staff will use school provided equipment. If this is not available, staff will only use personal devices with prior approval from the headteacher following a formal risk assessment. Staff will follow clear guidance outlined in the Acceptable Use Policy.
- If a member of staff breaches our policy, action will be taken in line with our staff behaviour policy/code of conduct, child protection policy and/or allegations policy.
- If a member of staff is thought to have illegal content saved or stored on a personal mobile or other device or 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 allegations policy.

6. Pupils use of mobile and smart technology.

- Pupils 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 pupils as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources.
- Personal mobile or smart technology devices are not to be used on site by pupils. The only exception to this is:
 - Staff will only allow certain pupils to use their personal mobile or smart devices as part of an educational visit, following a risk assessment, with approval from the Leadership Team.
- City of Rochester school expects pupils' personal mobile or smart devices to be kept safe and secure when on site. This means:
 - \circ ~ handing into the school office at the start of day, switched off.

Page 3 of 6

- If a learner needs to contact their parents or carers whilst on site, they will be allowed to use a school phone.
- If a learner requires access to a personal mobile or smart device in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with the headteacher prior to use being permitted.
 - Any arrangements regarding access to personal mobile or smart devices in exceptional circumstances will be documented and recorded by the school.
 - 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 pupils' personal mobile or smart devices are used when learning at home, this will be in accordance with our Acceptable Use Policy.
- Personal mobile or smart devices must not be taken into examinations. Pupils 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.

6.1 Searching, screening and confiscation of electronic devices

- Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.
- Where there are any concerns regarding pupils' use of mobile or smart technology or policy breaches, they will be dealt with in accordance with our existing policies, including anti-bullying, child protection, online safety and behaviour.
- Staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene our child protection or behaviour policy.
- Personal mobile or smart technology devices that have been confiscated will be held in a secure place, in the school office and released to parents/carers.
- Where a concern involves a potentially indecent image or video of a child, staff will respond in line with our child protection policy and will confiscate devices, avoid looking at any content, and refer the incident to the Designated Safeguarding Lead (or deputy) urgently as they will be most appropriate person to respond.
- If there is suspicion that data or files on a pupils personal mobile or smart technology devices may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.
- If deemed to be necessary and appropriate, searches of personal mobile or smart technology devices may be carried out in accordance with our behaviour policy and the DfE <u>'Searching, Screening and</u> <u>Confiscation'</u> guidance.
- Staff will respond in line with our child protection policy and follow the most appropriate safeguarding response if they find images, data or files on a pupil's electronic device that they reasonably suspect are likely to put a person at risk.
- The Designated Safeguarding Lead (or deputy) will always be informed of any searching incidents where authorised members of staff have reasonable grounds to suspect a pupil was in possession of prohibited items, as identified in our behaviour policy.
- The Designated Safeguarding Lead (or deputy) will be involved without delay if staff believe a search of a pupil's personal mobile or smart technology device has revealed a safeguarding risk.

Page 4 of 6

- In exceptional circumstances and in accordance with our behaviour policy and the DfE <u>'Searching,</u> <u>Screening and Confiscation'</u> guidance, the headteacher or authorised members of staff may examine or erase data or files if there is a good reason to do so.
- If the headteacher or a member of staff finds any data or files that they suspect might constitute a specified offence, they will be delivered to the police as soon as is reasonably practicable.

7. Visitors' use of mobile and smart technology

- Parents/carers and visitors, including volunteers and contractors, are expected to ensure that:
 - Personal devices e.g., mobile phones, tablets, smart devices, cameras must NOT be used in school or around the children and should be switched off on entering the building.
- Appropriate information is in place to inform visitors of our expectations for safe and appropriate use of personal mobile or smart technology devices.
- 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 our acceptable use of technology policy and other associated policies, including child protection.
- If visitors require access to mobile and smart technology, for example when working with pupils as part of multi-agency activity, this will be discussed with the headteacher prior to use being permitted.
 - Any arrangements regarding agreed visitor access to mobile/smart technology will be documented and recorded by the school. 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 or headteacher of any breaches of our policy.

8. Policy monitoring and review

- Technology evolves and changes rapidly. City of Rochester school will review this policy 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.
- We monitor internet and technology use taking place via all City of Rochester provided devices and systems and regularly evaluate online safety mechanisms to ensure this policy is consistently applied. Full information about the appropriate filtering and monitoring systems in place are detailed in our child protection policy. Any issues identified as a result of our monitoring approaches will be incorporated into our action planning.
- All members of the community will be made aware of how the City of Rochester will monitor policy compliance.

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 school policies and procedures.
- Where pupils breach this policy:
 - $\circ\,$ appropriate sanctions and/or pastoral/welfare support will be implemented in line with our behaviour policy.
 - o concerns will be shared with parents/carers as appropriate.
 - we will respond in line with our child protection policy, if there is a concern that a child is at risk of harm.
- 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 pupils to work in partnership with us to resolve issues.

Page 5 of 6

- All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.
- Pupils, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- If we are unsure how to proceed with an incident or concern, the DSL (or a deputy) or headteacher will seek advice from Medway or Kent County Councils Education Safeguarding Service or other agency in accordance with our child protection policy.

City of Rochester School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is out aim that all pupils fulfil their potential.

Page 6 of 6