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 will be subject to continuous monitoring, refinement and audit by the Headteacher
- The Trustees undertake a formal review of this policy for the purpose of monitoring and of the efficiency with which the related duties have been discharged, by no later than one year from the date shown below, or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so requires. This discussion will be formally documented in writing. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay.

Signed:

Date Reviewed: September 2022

Date of Next Review: September 2023

Version No. 2

Alicja Emmett

Claire Cooper

Headteacher Chair of Trustees and Safeguarding Trustee

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 The Education People's mobile and smart technology policy template with specialist advice and input as required, taking into account the DfE statutory guidance 'Keeping Children Safe in Education' 2022, 'Working Together to Safeguard Children' 2018 'Behaviour in Schools Advice for headteachers and school staff' 2022, 'Searching, screening and confiscation at school' 2022 and the local Medway Safeguarding **Children Board** (MSCB) procedures.
- The purpose of this policy is to safeguard and promote the welfare of all members of City of Rochester community when using mobile devices and smart technology.
 - The 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.
 - o As outlined in our Child Protection Policy, the Designated Safeguarding Lead (DSL), Michelle Homer, 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 mobile 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).

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
 - 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
 - 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.
- Mobile phones, digital music players, smart watches and other personal electronic devices have become more widely available.
- As a school we must make a sensible and practical response. We understand that parents wish their child
 to carry a mobile phone for their personal safety, whilst young people may wish to bring additional
 devices to the school for other reasons.
- Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of the school community are advised to:
 - o 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.
 - o use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on their phones or devices.
- Mobile phones and personal devices are not permitted to be used in specific areas on site, classrooms and in meetings.
- The sending of abusive or inappropriate messages or content, including via personal smart devices and mobile phones 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 school 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 child protection policies.

4. School/setting-provided 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.
- School devices will always be used in accordance with the acceptable use of technology policy and other relevant policies.
- Where staff and/or pupils are using school 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.

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 school policy and procedures, such as confidentiality, child protection, data security staff behaviour/code of conduct and Acceptable Use Policies.
- Staff will be advised to:
 - Keep mobile phones and personal devices in a safe and secure place during lesson time.
 - o 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 headteacher, such as in emergency circumstances.
 - 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 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):
 - o to take photos or videos of pupils in line with our image use policy.
 - to work directly with pupils during lessons/educational activities.
 - o 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 code of conduct and allegations policy.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal
 device or have committed a criminal offence 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.
- Mobile phones and/or personal devices will not be used on site by pupils. The only exception to this is:
 - Staff will only allow certain pupils to use their mobile phones or personal devices as part of an educational visit, following a risk assessment, with approval from the Leadership Team.
- City of Rochester school expects pupils' personal devices and mobile phones to be kept safe and secure when on site. This means:
 - o handing into the school office at the start of day, switched off.
- 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 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 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' mobile phones or personal devices are used when learning at home, this will be in accordance with our Acceptable Use Policy.
- Mobile phones and personal 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.
- Any concerns regarding pupils use of mobile technology or policy breaches will be dealt with in accordance with our existing policies, including anti-bullying, child protection and positive behaviour.
 - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our child protection, behaviour or anti-bullying policy.
 - Searches of mobile phone or personal devices will be carried out in accordance with our policy.
 - Pupils' mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/carer. Content may be deleted or requested to be deleted if it contravenes our policies.
 - Mobile phones and devices that have been confiscated will be held in a secure place and released to parents/carers.
 - Appropriate sanctions and/or pastoral/welfare support will be implemented in line with our behaviour policy.
 - Concerns regarding policy breaches by pupils 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 child protection 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.

6.1 Screening, searching 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 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 pupils mobile phone or device if they believe it is being used to contravene our child protection or behaviour policy.
- Mobile phones and 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 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
- out in accordance with our behaviour policy and the DfE 'Searching, Screening and Confiscation' guidance. Link to appropriate policy and ensure your policy is in line with the DfE 'Searching, Screening and Confiscation' guidance. Link to appropriate policy and ensure your policy is in line with the DfE 'Searching, Screening and Confiscation' guidance. The headteacher or a member of staff authorised by the headteacher can carry out a search and examine any data or files on an electronic device confiscated as a result of a search, if there is good reason to do so. This would be where they have reasonable grounds for suspecting the device or content on the device poses a risk to staff and/or pupils, is prohibited, or identified in the school's behaviour policy for which a search can be made or is evidence in relation to an offence. The headteacher can authorise individual members of staff to search for specific items, or all items set out in the school's behaviour policy.
- 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 (link).
- The Designated Safeguarding Lead (or deputy) will be involved without delay if staff believe a search of a pupil's device has revealed a safeguarding risk.
- In exceptional circumstances and in accordance with our behaviour policy (link) and the DfE 'Searching,
 <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. Ensure your policy is in line with the DfE 'Searching,
 <u>Screening and Confiscation'</u> guidance. The DfE 'Searching, Screening and Confiscation' guidance states
 (77 79)
 - In determining whether there is a 'good reason' to examine images, data or files, the headteacher or an authorised member of staff will need to reasonably suspect that the images, data or files on

- the device has been, or could be used, to cause harm, undermine the safe environment of the school and disrupt teaching, or be used to commit an offence.
- O In determining whether there is a 'good reason' to erase any images, data or files from the device, the member of staff should consider whether the material found may constitute evidence relating to a suspected offence. In those instances, the data or files should not be deleted, and the device must be handed to the police as soon as it is reasonably practicable.
- If the data or files are not suspected to be evidence in relation to an offence, the headteacher or an authorised member of staff may delete the images, data or files if the continued existence of the data or file is likely to continue to cause harm to any person and the pupil and/or the parent refuses to delete the data or files themselves.
- 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, cameras and ipods 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 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 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 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. Any issues identified will be
 incorporated into our action planning.

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:
 - o 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.
- 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 the LADO or other agency in accordance with our child protection policy.