Tenax Schools Trust

Acceptable Use, Mobile Technology and Social Media Policy
September 2023

Adoption Arrangements and Date

All statutory policies in the Trust are ultimately the responsibility of the Trust Board. To enable it to discharge this responsibility appropriately and in collaboration with the constituent schools, the Trust Board will either

1. set a full Trust wide policy which applies in the same way to all schools
2. require individual schools to set a policy (in most cases with Trust-provided guidance) appropriate to the needs and circumstances of an individual school

Author:	Trust Primary School Executive DSL	**Adopted:**	**12 September 2023**
		Adopted:	**12 September 2023**
Leadership Grp Responsibility: CEO		**Date of next review:**	**August 2026**
Policy Type:	**Statutory**	**Review period:**	**3 year or in response to new national guidance**

This is a Level 2 Policy against the Trust Governance Plan.

Key Contact Personnel in School

Role	Name	Contact Details
School Designated Safeguarding Lead (DSL)	Tina Holditch	headteacher@leybourne.school
School Deputy Safeguarding Lead(s)	Louise Grinstead Kerri Miller	lgrinstead@leybourne.school kmiller@leybourne.school
Nominated governor for safeguarding and child protection	Philippa Gibbs	Via clerk to the Governors swallis@leybourne.school
Chair of the Local Governing Body	Andy Rathbone	[via clerk to the trustees] clerk@tenaxschoolstrust.co.uk
Trust Primary School Executive DSL	Matthew Clark	07383 518543 clark@tenaxschoolstrust.co.uk
Nominated Trustee for safeguarding and child protection	Andy Rathbone	[via clerk to the trustees] clerk@tenaxschoolstrust.co.uk

Acceptable Use of Technology for Staff, Visitors and Volunteers

Staff Acceptable Use of Technology Policy (AUP)

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Leybourne SS Peter and Paul CEP Academy's IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for pupils, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand Leybourne SS Peter and Paul CEP Academy's expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that school systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy scope

1. I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within Leybourne SS Peter and Paul CEP Academy both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning and online and offline communication technologies**.**

2. I understand that Leybourne SS Peter and Paul CEP Academy's Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school safeguarding and child protection policy, and staff code of conduct.

3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the school ethos, school staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of school devices and systems

4. I understand that any equipment and internet services provided by my workplace is intended for education purposes and/or professional use and should only be accessed by members of staff. Reasonable personal use of school IT systems and/or devices by staff is allowed.

Data and system security

5. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
    - I will use a 'strong' password to access school systems. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system.
    - I will protect the devices in my care from unapproved access or theft.

6. I will respect school system security and will not disclose my password or security information to others.

7. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT system manager and headteacher.

8. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.

9. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the school information security policies.
    - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
    - Any data being removed from the school site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the school.

10. I will not keep documents which contain school related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school's approved platform to upload any work documents and files in a password protected environment.

11. I will not store any personal information on the school IT system, including school laptops or similar device issued to members of staff, that is unrelated to school activities, such as personal photographs, files or financial information.

12. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

13. I will not attempt to bypass any filtering and/or security systems put in place by the school.

14. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT system manager and headteacher as soon as possible.

15. If I have lost any school related documents or files, I will report this to the Headteacher and the Trust's Data Protection Officer as soon as possible.

16. Any images or videos of pupils will only be used as stated in the school camera and image use policy (link). I understand images of pupils must always be appropriate and should only be taken with school provided equipment and only be taken/published where pupils and/or parent/carers have given explicit written consent.

Classroom practice

17. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in the safeguarding and child protection policy and in the policy attached to this AUP.

18. I have read and understood the school mobile and smart technology and social media policies.

19. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
    - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
    - creating a safe environment where pupils feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
    - involving the Designated Safeguarding Lead (DSL) or a deputy as part of planning online safety lessons or activities to ensure support is in place for any pupils who may be impacted by the content.
    - make informed decisions to ensure any online safety resources used with pupils is appropriate.

20. I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL in line with the school safeguarding and child protection policy.

21. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, or distribute or use them.

Mobile devices and smart technology

22. I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the staff code of conduct and the school mobile technology policy and the law.

Online communication, including use of social media

23. I will ensure that my use of communication technology, including use of social media is compatible with my professional role, does not interfere with my work duties and takes place in line with the safeguarding and child protection policy and staff code of conduct, social media policy and the law.

24. As outlined in the staff code of conduct and this policy:
    - I will take appropriate steps to protect myself and my reputation, and the reputation of the school, online when using communication technology, including the use of social media.
    - I will not discuss or share data or information relating to pupils, staff, school business or parents/carers on social media.

25. My electronic communications with current and past pupils and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
    - I will ensure that all electronic communications take place in a professional manner via school approved and/or provided communication channels and systems, such as a school email address, user account or telephone number.
    - I will not share any personal contact information or details with pupils, such as my personal email address or phone number.
    - I will not add or accept friend requests or communications on personal social media with current or past pupils and/or their parents/carers.
    - If I am approached online by a current or past pupils or parents/carers, I will not respond and will report the communication to my line manager and Designated Safeguarding Lead (DSL).
    - Any pre-existing relationships or situations that compromise my ability to comply with the AUP or other relevant policies will be discussed with the DSL and/or headteacher.

Policy concerns

26. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.

27. I will not attempt to access, create, transmit, display, publish or forward any material or content online that may be harmful, inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

28. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.

29. I will report and record any concerns about the welfare, safety or behaviour of pupils or parents/carers online to the DSL in line with the school child protection policy.

30. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with school child protection policy and the allegations against staff policy.

Policy Compliance and Breaches

31. If I have any queries or questions regarding safe and professional practise online, either in school or off site, I will raise them with the DSL and the headteacher.

32. I understand that the school may exercise its right to monitor the use of its information systems, including internet access and the interception of messages/emails on our systems, to monitor policy compliance and to ensure the safety of pupils and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

33. I understand that if the school believe that unauthorised and/or inappropriate use of school systems or devices is taking place, the school may invoke its disciplinary procedures as outlined in the staff code of conduct.

34. I understand that if the school believe that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures as outlined in the staff code of conduct.

35. I understand that if the school suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with the Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of staff member: ……

Signed: ……

Date (DDMMYY)……..

The use of mobile and smart devices

1. Policy aims and scope

- This policy has been written by Leybourne SS Peter and Paul CEP Academy, involving staff, pupils and parents/carers, building on Kent County Council's 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 'Keeping Children Safe in Education', Early Years and Foundation Stage, 'Working Together to Safeguard Children', 'Behaviour in Schools Advice for headteachers and school staff', 'Searching, screening and confiscation at school' and the local Kent Safeguarding Children Multi-agency Partnership (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.
    - Leybourne SS Peter and Paul CEP Academy 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), Tina Holditch, Headteacher, 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 governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (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:
    - Acceptable Use Policies (AUP)
    - Behaviour and discipline policy
    - Cameras and image use policy
    - Child protection policy
    - Staff code of conduct
    - Confidentiality policy

- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- Data security
- Social media

3. Safe use of mobile and smart technology expectations

- Leybourne SS Peter and Paul CEP Academy 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 classrooms when pupils are changing, and toilets.
- 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 Leybourne SS Peter and Paul CEP Academy 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. School provided mobile phones and devices

- Staff providing formal remote/online learning will do so using school provided equipment in accordance with our Acceptable Use Policy (AUP)/remote learning AUP.
- School devices (laptops or iPads) will be suitably protected via a passcode/password/PIN and must only be accessed or used by members of staff and/or pupils.
- School 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 are using school provided 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, 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 personal 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 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 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/students 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/or headteacher.
- Staff will only use school provided equipment (not personal devices):
    - 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 and/or remote learning AUP.
- 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. Further information is contained within our child protection and relevant specific curriculum policies, for example, RSE and Computing.
- Pupils are not permitted to use personal mobile or smart devices whilst on the school site. Where these are required, for example for safety reasons when children/young people are transporting to and from school, devices should be turned off/placed on silent and handed into the class teacher in the morning. They can then be collected at the end of day.
- If a child needs to contact their parents or carers whilst on site, they will be allowed to use the office phone. Parents are advised to contact their child via the school office; exceptions may be permitted on a case-by-case basis, as approved by the headteacher.
- If a child/pupil/student requires access to personal mobile or smart technology devices in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with the headteacher prior to use being permitted.
- 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 technology devices are used when learning at home, this will be in accordance with our Acceptable Use Policy and/or Remote Learning AUP.
- Personal mobile or smart technology 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 child's/pupils/students' personal mobile or smart technology 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 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 child/pupils/student's personal mobile or smart technology device 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 '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.
- 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.
- In exceptional circumstances and in accordance with our behaviour policy and the DfE 'Searching, Screening and Confiscation' guidance, the headteacher or authorised members of staff may examine or erase data or files if there is a good reason to do so.
    - 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.
    - 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 mobile phones are used for explicit purposes and in agreed circumstances.
- Appropriate signage and information are in place to inform visitors of our expectations for safe and appropriate use of personal mobile or smart technology.
- 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 / headteacher of any breaches of our policy.

8. Policy monitoring and review

- Technology evolves and changes rapidly. Leybourne SS Peter and Paul CEP Academy 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 school 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 school will monitor policy compliance, for example through AUPs, staff training, classroom management.

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. This includes the child protection and behaviour policies.
- Where pupils breach this policy:
    - appropriate sanctions and/or pastoral/welfare support will be implemented in line with our behaviour policy.
    - 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 Trust Executive Designated Safeguarding Lead, Kent County Councils Education Safeguarding Service or other agency in accordance with our child protection policy.

Social Media Policy

1. Policy aims and scope

- This policy has been written by Leybourne SS Peter and Paul CEP Academy, 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 'Keeping Children Safe in Education', Early Years and Foundation Stage, 'Working Together to Safeguard Children', 'Behaviour in Schools Advice for headteachers and school staff', 'Searching, screening and confiscation at school' and the local Kent Safeguarding Children Multi-agency Partnership (KSCMP) procedures.
- The purpose of this policy is to safeguard and promote the welfare of all members of the Leybourne SS Peter and Paul CEP Academy community when using social media.
    - Leybourne SS Peter and Paul CEP Academy 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 social media.
    - As outlined in our child protection policy, the Designated Safeguarding Lead (DSL), Tina Holditch, Headteacher, 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 pupils, 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 school (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:
    - Acceptable Use Policies (AUP)
    - Behaviour and discipline policy
    - Cameras and image use policy
    - Child protection policy
    - Staff code of conduct/staff behaviour policy
    - Confidentiality policy
    - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)

- Data security
- Mobile and smart technology
- Online Safety

3. General social media expectations

- Leybourne SS Peter and Paul CEP Academy believes everyone should be treated with kindness, respect and dignity. Even though online spaces may differ in many ways, the same standards of behaviour are expected online as offline, and all members of our community are expected to engage in social media in a positive and responsible manner.
- All members of our community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.
- We will monitor and restrict learner and staff access to social media via our filtering and monitoring systems which are applied to all school provided devices and systems; further information on how this is achieved in addressed in our child protection policy.
- The use of social media or apps, for example as a formal remote learning platform or education tool will be robustly risk assessed by the DSL and/or headteacher prior to use with learners. Any use will take place in accordance with our existing policies, for example, child protection, staff/learner behaviour acceptable use policies, remote learning Acceptable Use Policy.
- Concerns regarding the online conduct of any member of Leybourne SS Peter and Paul CEP Academy community on social media will be taken seriously. Concerns will be managed in accordance with the appropriate policies, including anti-bullying, allegations against staff, behaviour, home school-agreements, staff behaviour/code of conduct, Acceptable Use Policies, and child protection.

4. Staff use of social media

- The use of social media during school hours for personal use is permitted for staff, during break periods.
- Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our code of conduct/behaviour policy and acceptable use of technology policy.
- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction. Advice will be provided and updated via staff training and additional guidance and resources will be shared with staff as required on a regular basis.
- Any complaint about staff misuse of social media or policy breaches will be taken seriously in line with our child protection and allegations against staff policy.

4.1 Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school. Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media. This may include, but is not limited to:
    - School appropriate privacy levels on their personal accounts/sites.
    - Being aware of the implications of using location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Using strong passwords.
    - Ensuring staff do not represent their personal views as being that of the school.
- Members of staff are encouraged not to identify themselves as employees of Leybourne SS Peter and Paul CEP Academy on their personal social networking accounts; this is to prevent information being linked with the school and to safeguard the privacy of staff members.
- All staff are expected to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional reputation and legal framework. All members of staff are encouraged to carefully consider the information, including text and images, they share and post on social media.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues, will not be shared or discussed on social media sites.
- Members of staff will notify the leadership team immediately if they consider that any content shared on social media sites conflicts with their role.

4.2 Communicating with pupils and their families

- Staff will not use any personal social media accounts to contact pupils or their family members.
- All members of staff are advised not to communicate with or add any current or past pupils or their family members, as 'friends' on any personal social media accounts.
- Any communication from pupils and parents/carers received on personal social media accounts will be reported to the headteacher.
- Any pre-existing relationships or situations, which mean staff cannot comply with this requirement, will be discussed with the headteacher. Decisions made and advice provided in these situations will be formally recorded to safeguard pupils, members of staff and the school.
- If ongoing contact with pupils is required once they have left the school, members of staff will be expected to use existing alumni networks, or use official school provided communication tools.

5. Pupils' use of social media

- The use of social media during school hours for personal use is not permitted for children.
- Many online behaviour incidents amongst children and young people occur on social media outside the school day and off the school premises. Parents/carers are responsible for this behaviour; however, some online incidents may affect our culture and/or pose a risk to children and young people's health and well-being. Where online behaviour online poses a threat or causes harm to another child, could have repercussions for the orderly running of the school when the child is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school, action will be taken in line with our behaviour and child protection/online safety policies.
- Leybourne SS Peter and Paul CEP Academy will empower our pupils to acquire the knowledge needed to use social media in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks. Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection and relevant specific curriculum policies, for example, RSE and Computing.
- We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for pupils under the required age as outlined in the services terms and conditions.
- Pupils will be advised:
    - to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location.
    - to only approve and invite known friends on social media sites and to deny access to others, for example by making profiles private.
    - not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present.
    - to use safe passwords.
    - to use social media sites which are appropriate for their age and abilities.
    - how to block and report unwanted communications.
    - how to report concerns on social media, both within the school and externally.
- Any concerns regarding pupils' use of social media will be dealt with in accordance with appropriate existing policies, including anti-bullying, child protection and behaviour.
- The DSL (or deputy) will respond to social media concerns involving safeguarding or child protection risks in line with our child protection policy.
- Sanctions and/or pastoral/welfare support will be implemented and offered to pupils as appropriate, in line with our child protection and behaviour policy. Civil or legal action may be taken if necessary.

- Concerns regarding pupils' use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

6. Policy monitoring and review

- Technology evolves and changes rapidly. Leybourne SS Peter and Paul CEP Academy 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.

7. 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.
- 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 headteacher/DSL (or a deputy) will seek advice from the Trust Executive Safeguarding Lead, Kent County Council's Education Safeguarding Service or other agency in accordance with our child protection policy.