Viking Academy Trust

Acceptable Use Policy (Staff, parents, learners and Visitors/Volunteers)

Approved by the Trust: Term 2 2019

Reviewed annually: Term 1

Last review date: Term 1 2021

Signed **Chair of Trust**

Acceptable Use Policy (staff and volunteers)

The Viking Academy Trust

Empowering Children Through Education: One Childhood One Chance

Schools in the Viking Academy Trust (VAT)

Chilton Primary School
Ramsgate Arts Primary School
Upton Junior School

This 'Acceptable Use Policy' is specific to Chilton Primary school

Learner Acceptable Use of Technology Statements
Early Years and Key Stage 1

I understand that the Chilton Acceptable Use Policy will help keep me safe and happy online.

- I only use the internet when an adult is with me.
- I only click on links and buttons online when I know what they do.
- I keep my personal information and passwords safe.
- I only send messages online which are polite and friendly.
- I know the school can see what I am doing online when I use school computers and tablets and name of any specific school systems learners are expected to use, including when I am at home.
- I always tell an adult if something online makes me feel upset, unhappy, or worried.
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online.
- I know that if I do not follow the rules:
    - My parents will be informed
    - I may not be permitted to use school devices
    - I may lose behaviour points
- I have read and talked about these rules with my parents/carers.

Key Stage 2

I understand that the school Acceptable Use Policy will help keep me safe and happy online at home and at school

Safe

- I will behave online the same way as I behave in the classroom.
- I only send messages which are polite and friendly.
- I will only post pictures or videos on the internet if they are safe and appropriate, and if I have permission.
- I only talk with and open messages from people I know.

- I will only click on links if I know they are safe.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.

Learning

- I know I must not use my personal device at school
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher or teaching assistant has chosen.
- I use school devices for school work unless I have permission otherwise.
- If I need to learn online at home, I will follow the school rules for acceptable use and follow the behaviour policy

Trust

- I know that not everything or everyone online is honest or truthful.
- I will check content on other sources like other websites, books or with a trusted adult.
- I always credit the person or source that created any work, images, or text I use.

Responsible

- I keep my personal information safe and private online.
- I will keep my passwords safe and will not share them.
- I will not access or change other people's files or information.
- I will only change the settings on a device if a member of staff has allowed me to.
- If I am in Year 5 or 6 and have to bring my phone to school because I walk to school by myself, I know I must leave my phone in the school office at the start of the day and collect it again when I leave school

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that all school devices and systems are monitored to help keep me safe, including when I use them at home.
- I have read and talked about these rules with my parents/carers.
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online.
- I know that if I do not follow the school rules then:
  - My parents will be informed
  - I may not be allowed to use devices and/or the internet
  - I may lose behaviour points
  - I may have to miss a break time

Tell

- If I see anything online that I should not or that makes me feel worried or upset, I will minimise the page and tell an adult straight away. I will close a lap top lid or press the home screen button on an ipad.
- If I am aware of anyone being unsafe with technology, I will report it to a teacher.
- I know it is not my fault if I see or someone sends me something bad online. I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened

- I ask a grown up if I want to use the computer
- I make good choices on the computer
- I use kind words on the internet
- If I see anything that I do not like online, I tell a grown up
- I know that if I do not follow the school rules then:
    - My parents will be informed
    - I may lose a treat / choice
    - I may lose behaviour points

Learners with SEND functioning at Levels P7-L1

(Based on Childnet's SMART Rules: www.childnet.com)

Safe

- I ask a grown up if I want to use the computer
- I do not tell strangers my name on the internet
- I know that if I do not follow the school rules then:
    - My parents will be informed
    - I may lose a treat / choice
    - I may lose behaviour points

Meeting

- I tell a grown up if I want to talk on the internet

Accepting

- I do not open messages or emails from strangers

Reliable

- I make good choices on the computer

Tell

- I use kind words on the internet
- If I see anything that I do not like online, I will tell a grown up

Acceptable Use of Technology Form for Parents/Carers

Chilton Primary School Learner Acceptable Use of Technology Policy Acknowledgment

1. I, with my child, have read and discussed Chilton's learner acceptable use of technology policy (AUP) and understand that the AUP will help keep my child safe online.
2. I understand that the AUP applies to my child use of school devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns.
3. I am aware that any use of school devices and systems may be monitored for safety and security reason to keep my child safe and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
4. I am aware that the school mobile technology policy states that my child cannot use personal device and mobile technology on site.
5. I understand that my child needs a safe and appropriate place to access remote learning if school is closed in response to Covid-19. I will ensure my child's access to remote learning is appropriately supervised.
6. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use school devices and systems. I understand that the school cannot

ultimately be held responsible for the nature and content of materials accessed on the internet or if my child is using mobile technologies.

7. I with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.
8. I understand that the school will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety.
9. I will inform the school or other relevant organisations if I have concerns over my child's or other members of the school communities' safety online.
10. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school
11. I will support the school online safety approaches. I will use appropriate parental controls and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

Form will be sent electronically to be signed and record kept of responses

Staff Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Chilton Primary School 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 learners, 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 Chilton Primary School 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 Chilton Primary School 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 Chilton Primary School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school staff code of conduct and remote learning Policy
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 will only use the equipment and internet services provided to me by the school for example school provided laptops, tablets, mobile phones, and internet access, when working with learners.
5. 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.
6. Where I deliver or support remote learning, I will comply with the school remote learning policy.

Data and System Security

7. 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. I will not leave a device unsupervised or visible in a public place.

8. I will respect school system security and will not disclose my password or security information to others.
9. 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 Team
10. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT Team
11. 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 Sharepoint will be suitably password protected

12. 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. I will use the school learning platform (Sharepoint or OneDrive) to upload any work documents and files in a password protected environment
13. 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.
14. 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.

15. I will not attempt to bypass any filtering and/or security systems put in place by the school.
16. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the IT Team (Jarvis Deveson, Nick Barfoot)
17. If I have lost any school related documents or files, I will report this to the IT Team (Jarvis Deveson, Nick Barfoot) and school Data Protection Officer (Lisa Blatchford) as soon as possible.
18. Any images or videos of learners will only be used as stated in the school image use policy. I understand images of learners must always be appropriate and should only be taken with school provided equipment and only be taken/published where learners and/or parent/carers have given explicit written consent.

Classroom Practice

19. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in: Child Protection, AUP, Use of mobile and smart technology policies and code of conduct
20. I have read and understood the school mobile technology and social media policies.
21. I will promote online safety with the learners 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 learners 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) (Kate Law) or a deputies (Natalie Barrow and Hannah Cheshire) as part of planning online safety lessons or activities to ensure support is in place for any learners who may be impacted by the content.
- make informed decisions to ensure any online safety resources used with learners is appropriate.

22. I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL in line with the school child protection policies.
23. 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

24. 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

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

26. My electronic communications with current and past learners 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 learners, 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 learners and/or their parents/carers.
- If I am approached online by a current or past learner or parents/carer, 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 will be discussed with the DSL

Policy Concerns

27. 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.
28. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.
29. 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.
30. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the DSL in line with the school child protection policy.
31. I will report concerns about the welfare, safety, or behaviour of staff to the Head of School, in line with the allegations against staff policy

Policy Compliance and Breaches

32. 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
33. I understand that the school may exercise its right to monitor the use of its information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
34. I understand that if the school believes 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 code of conduct
35. I understand that if the school believes 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 code of conduct. 36. I understand that if the school suspects criminal offences have occurred, the police will be informed.