Staff Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use The Craylands 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 The Craylands School'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 The Craylands 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 The Craylands School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school staff behaviour policy/code of conduct and remote learning AUP (appendix a).

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 <mark>education purposes and/or professional use</mark> and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed.

   Occasional personal use of the settings devices could be considered as beneficial to the development of staff IT skills and can enable staff to maintain a positive work-life balance.

6. Where I deliver or support remote learning, I will comply with the school remote learning AUP.

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.

   o 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.*

   o I will protect the devices in my care from unapproved access or theft e.g. *not leaving devices visible or unsupervised in public places.*

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 system manager.

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

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.

    o 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.
> - o Any data being removed from the school site, such as via email will be suitably 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. Where possible, I will use the school network or one drive to save documents suitably protected.

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 ICT Technician as soon as possible.

17. If I have lost any school related documents or files, I will report this to the school Data Protection Officer (Kris Hiscock) as soon as possible.

18. Any images or videos of learners will only be used as stated in the school camera and 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, online safety, remote learning AUP.

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:

   o exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
   o 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.
   o involving the Designated Safeguarding Lead (DSL) (Kylie Cox) or a deputy (Lisa Farrell, Leanne Drake, Yvonne Stone, Kris Hiscock) 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.
   o 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 behaviour policy/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 staff behaviour policy/code of conduct, the school social media policy and the law. In line with the school social media policy:

- o   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.
- o   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.

- o   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.
- o   I will not share any personal contact information or details with learners, such as my personal email address or phone number.
- o   I will not add or accept friend requests or communications on personal social media with current or past learners and/or their parents/carers.
- o   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).
- o   Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the DSL and/or headteacher

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 headteache, in line with the allegations against staff policy.

The Craylands School

Acceptable Use Policy for Staff

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 and/or the headteacher.

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 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 behaviour policy/code of conduct.

35. 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 behaviour policy/code of conduct.

36. 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 Craylands School 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)……………………………………………………………………………………...

Appendix A

Staff Remote Learning AUP

The Remote Learning Acceptable Use Policy (AUP) is in place to safeguarding all members of school community when taking part in remote learning following any full or partial **school** closures.

Leadership Oversight and Approval
1. Remote learning will only take place using **Class Dojo/Zoom.**
   - **Class Dojo** has been assessed and approved by **the Headteacher.**

2. Staff will only use **school** managed **or** specific, approved professional accounts with learners **and/or** parents/carers.

   - Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.
     - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with **Kylie Cox,** Designated Safeguarding Lead (DSL).
   - Staff will use work provided equipment where possible **e.g. a school/setting laptop, tablet, or other mobile device.**

3. Online contact with learners **and/or** parents/carers will not take place outside of the operating times as defined by SLT:
   - **8.30a.m. and 4.30 p.m.**

4. All remote lessons will be decided upon by the class teacher.

5. Live-streamed remote learning sessions will only be held with approval and agreement from **the headteacher/a member of SLT.**

Data Protection and Security
6. Any personal data used by staff and captured by **Class Dojo** when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.

7. All remote learning and any other online communication will take place in line with current **school** confidentiality expectations.

8. Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by SLT and in line with our data protection policy requirements.

9. Only members of the The Craylands School community will be given access to **Class Dojo**.

10. Access to **Class Dojo** will be managed in line with current IT security expectations as outlined in **Online Safety policy**.

Session Management

11. Staff will record the attendance of any sessions held.
    Names of pupils attended will be sent to a member of SLT for records.

12. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
    - Use of waiting rooms
    - Users using their real names
    - Videos being switched on
    - Disable access by children to share screen etc

13. When live streaming with learners:
    - contact will be made via learners' **school** provided logins.
    - staff will **mute/disable** learners' videos and microphones.

14. Live 1:1 sessions will only take place with approval from the **headteacher/a member of SLT**.

15. A pre-agreed **invitation/email** detailing the session expectations will be sent to those invited to attend.
    - Access links should not be made public or shared by participants.
    - Learners **and/or** parents/carers should not forward or share access links.
    - If learners/parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
    - Learners are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.

16. Alternative approaches **and/or** access will be provided to those who do not have access e.g. school will loan DfE devices to parents/carers.

Behaviour Expectations

17. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
18. All participants are expected to behave in line with existing **school** policies and expectations. This includes:
    - Appropriate language will be used by all attendees.
    - Staff will not take or record images for their own personal use.
    - Other attendees can or cannot record events for their own use, and if so, any expectations or restrictions about onward sharing.

19. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
20. When sharing videos and/or live streaming, participants are required to:
    - wear appropriate dress.
    - ensure backgrounds of videos are neutral (blurred if possible).
    - ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.
21. Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches and Reporting Concerns

22. Participants are encouraged to report concerns during remote **and/or** live-streamed sessions:
    - Children should report concerns to the member of staff running the session
    - Children should tell a parent/carer
23. If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to **Kylie Cox (Assistant Head/DSL)**.
24. Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.
25. Sanctions for deliberate misuse may include:
    - restricting/removing use
    - contacting police if a criminal offence has been committed.
26. Any safeguarding concerns will be reported to **Kylie Cox** Designated Safeguarding Lead, in line with our child protection policy.

I have read and understood the The Craylands School Acceptable Use Policy (AUP) for remote learning.

Staff Member Name: …………………………………………………………………………….

Date……………………………………………………………………………………………..

Appendix B

Early Years and Key Stage 1

I understand that the school 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 including when I am at home.
- I always tell an adult/teacher/member of staff 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/carers will be spoken to
  - I may not be allowed to use the computer
  - I may be put on the red face/receive a red card for not following instructions
- I have read and talked about these rules with my parents/carers.

The Craylands School

Acceptable Use Policy for Staff

Key Stage 2 (7-11)

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 always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher 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 schoolremote learning AUP.

Trust
- I know that not everything or everyone online is honest or truthful.
- I will check content on various 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.

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/carers may be spoken to
    - I may receive a warning or consequence card depending on the severity of the rule breaking
    - I may not be able to use online technology for the remainder of the lesson

Tell

- If I see anything online that I should not or that makes me feel worried or upset, I will minimise the page and/or turn off the screen and tell an adult straight away.
- 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.