Nurturing to Learn

ACCEPTABLE USE POLICY

This policy will be reviewed **at least** annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures.

Student Acceptable Use of Technology Statements

Key Stage 1

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

- I only go online with a grown-up.
- I am kind online.
- I keep information about me safe online.
- I tell a grown-up if something online makes me unhappy or worried.
- I know that if I do not follow the rules I will not be allowed to use computers to a period of time.
- 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.

- When I bring a personal/smart device and/or mobile phone into school I know that it is to be handed in to my teacher and then collected at the end of the school day.
- I know that all school devices/computers and systems are monitored, including when I am using them at home.
- I will tell a teacher or other adult if someone online makes me feel uncomfortable or worried when I am online using games or other websites or apps.

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 am not allowed to use my own personal smart devices and/or mobile phone at school.
- 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 school remote/online 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 rules I will not be allowed to use computers to a period of time.

Tell

- If I see anything online that I should not or that makes me feel worried or upset, I will **shut the laptop lid, turn off the screen**.
- 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.

Key Stage 3 and 4

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

- I know that school computers, tablets, laptops, and internet access has been provided to help me with my learning and that other use of technology may not be allowed. If I am not sure if something is allowed, I will ask a member of staff.
- I know that my use of school computers and devices, systems and on-site internet access will be monitored to keep me safe and ensure policy compliance.
- I know that if the school suspect that I am behaving inappropriately with technology, then enhanced monitoring approaches may be used, such as checking and/or confiscating personal technologies such as mobile phones and other devices.
- I know that if I do not follow the rules I will not be allowed to use computers to a period of time.
- If I am aware of anyone trying to misuse technology, I will report it to a member of staff.
- I have read and talked about these rules with my parents/carers.

Learning

- I know that school computers, devices and internet access has been provided to help me with my learning and that other use of technology may not be allowed. If I am not sure if something is allowed, I will ask a member of staff.
- If I need to learn online at home, I will follow the school remote learning AUP.
- I will not use my personal device/mobile phone in school.

Safe

- I will make sure that my internet use is safe and legal, and I am aware that online actions have offline consequences.
- I know that my use of school devices and systems will be monitored, at home and at school, to protect me and to ensure I comply with the acceptable use policy.
- I know that people online are not always who they say they are and that I must always talk to an adult before meeting any online contacts.

Private

- I will keep my passwords private.
- I know I must always check my privacy settings are safe and private.
- I will think before a share personal information **and/or** seek advice from an adult.
- I will keep my password safe and private as my privacy, school work and safety must be protected.

Responsible

- I will not access or change other people files, accounts, or information.
- I will only upload appropriate pictures or videos of others online and when I have permission.
- I know I must respect the school systems and equipment and if I cannot be responsible then I will lose the right to use them.
- I will write emails and online messages carefully and politely as I know they could be forwarded or seen by someone I did not intend.
- I will only change the settings on the computer if a teacher/technician has allowed me to.
- I know that use of the school ICT system for personal financial gain, gambling, political purposes, or advertising is not allowed.
- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that if the school suspect that I am behaving inappropriately with technology, then enhanced monitoring approaches may be used, such as checking and/or confiscating personal technologies such as mobile phones and other devices.
- I know that if I do not follow the rules I will not be allowed to use computers to a period of time.

Kind

- I know that bullying in any form (on and offline) is not tolerated; technology should not be used for any form or abuse or harassment.
- I will not upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.
- I will always think before I post as text, photos or videos can become public and impossible to delete.
- I will not use technology to be unkind to people.

Legal

- I know cybercrime can be a criminal offence, for example gaining unauthorised access to systems (‘hacking’) and making, supplying or obtaining malware.
- I know it can be a criminal offence to send threatening and offensive messages.
- I will respect other people’s information and copyright by giving a reference and asking permission before using images or text from online sources.

- I understand that it may be a criminal offence or breach of the school policy to download or share inappropriate pictures, videos, or other material online.
- I understand that it may be a criminal offence or a breach of the school policy to download or share inappropriate pictures, videos, or other material online. I understand that it is against the law to take, save or send nude or semi-nude images or videos of anyone under the age of 18.

Reliable

- I will always check that any information I use online is reliable and accurate.
- I know that people I meet online may not be who they say they are. If someone online suggests meeting up then I will immediately talk to an adult and will always arrange to meet in a public place, with a trusted adult present.

Report

- If I am aware of anyone trying to misuse technology, I will report it to a member of staff.
- I will speak to an adult I trust if something happens to either myself or another student which makes me feel worried, scared, or uncomfortable.
- I will visit www.thinkuknow.co.uk, www.childnet.com and www.childline.org.uk to find out more about keeping safe online.
- I have read and talked about these expectations with my parents/carers.

Pupil/Student Acceptable Use Policy Agreement Form

Elms School Acceptable Use of Technology Policy – Student Agreement

I, with my parents/carers, have read and understood the school Acceptable Use of Technology Policy (AUP) and remote learning AUP.

I agree to follow the AUP when:

1. I use school devices and systems both on site and at home.
2. I do not use my own devices in school.

Name……………………………………………. Signed…………………………….………...….

Class………………………………….………… Date…………………………………………….

Parent/Carer's Name……………………………………………...………......... (**If appropriate**)

Parent/Carer's Signature…………………………………………….………… (**If appropriate**)

Date………………………………………………………………………………………………

Acceptable Use of Technology Sample Statements and Forms for Parents/Carers

Parent/Carer AUP Acknowledgement Form

Student Acceptable Use of Technology Policy Acknowledgment

1. I have read and discussed Elms School student acceptable use of technology policy (AUP) with my child and understand that the AUP will help keep my child safe online.

2. I understand that the AUP applies to my child's use of school devices and systems on site and at home including (list devices/systems), and personal use where there are safeguarding and/or behaviour concerns. This may include if online behaviour poses a threat or causes harm to another student, could have repercussions for the orderly running of the school, if a student is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school.

3. I am aware that any use of school devices and systems are appropriately filtered and 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. This includes settings should inset appropriate information about the systems in place here.

4. I am aware that the school mobile and smart technology policy states that my child cannot use personal device and mobile and smart technology on site. Personal devices can be used on the buses for travel but must be handed into their class teacher or form tutor on arrival in school.

5. I understand that my child needs a safe and appropriate place to access remote/online learning, for example, if the school is closed in response to Covid-19. I will ensure my child's access to remote/online learning is appropriately supervised and any use is in accordance with the school remote learning AUP.

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 online or if my child is using personal mobile or smart technologies.

7. I and my child are aware of the importance of safe online behaviour and will not deliberately upload or share any content that could upset, threaten the safety of or offend any member of the school community, or content that could adversely affect the reputation of the school.

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 online.

9. I will inform the school (for example speaking to a member of staff and/or the Designated Safeguarding Lead) or other relevant organisations if I have concerns over my child's or other members of the school community's 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 understand my role and responsibility in supporting the school/settings online safety approaches and safeguarding my child online. I will use parental controls, supervise access and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

Child's Name………………………………….. Child's Signature ………………………………... (*if appropriate*)

Class……………………………………………. Date…………………………………………………………..

Parent/Carer's Name……………………………………………………………………………………….

Parent/Carer's Signature…………………………………………………………... Date……………………………

Acceptable Use of Technology for Staff, Visitors and Volunteers Sample Statements

Staff and Volunteer Acceptable Use of Technology Policy (AUP)

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Elms 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 students, 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 Elms 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 Elms 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 Elms School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school child protection, online safety policy , staff code of conduct and remote learning AUP.

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 students. **Staff can use personal devices away from the students for activities such as use of C-POM, school email or planning and preparation. These devices will be given an individual IP address when joining the wi-fi network, allowing the school to monitor the use of the devices and address any inappropriate use within school.**

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. Reasonable personal use of setting IT systems and/or devices by staff is allowed as o**ccasional 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. However, this is at the setting's discretion and can be revoked at any time. The use of the settings devices for personal social media is not allowed.**

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

7. **Data and system security**

8. 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.

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

10. 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.

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

12. 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.

13. 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 learning platform to upload any work documents and files in a password protected environment or school approved/provided VPN.

14. 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.

15. 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.

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

17. 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 Support Provider as soon as possible.

18. If I have lost any school related documents or files, I will report this to the ICT Support Provider and school Data Protection Officer as soon as possible.

19. Any images or videos of students will only be used as stated in the school camera. I understand images of students must always be appropriate and should only be taken with school provided equipment and only be published where students and/or parent/carers have given explicit written consent.

Classroom practice

20. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in insert names of relevant policies e.g. child protection, online safety, remote learning AUP.

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

22. I will promote online safety with the students 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 students 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 students who may be impacted by the content.
    - make informed decisions to ensure any online safety resources used with students is appropriate.

23. 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 and online safety policy.

24. 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

25. 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

26. 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 child protection, online safety policy, staff code of conduct, social media policy and the law.

27. As outlined in the staff code of conduct and school social media 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 students, staff, school business or parents/carers on social media.

28. My electronic communications with current and past students 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 students, 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 students and/or their parents/carers.
    - If I am approached online by a current or past students 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

29. 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.

30. 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.

31. 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.

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

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

Policy Compliance and Breaches

34. 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.

35. 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 students and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

36. 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.

37. 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.

38. 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 Elms 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)………………………………………………………………………………….…...

Visitor Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of our behaviour expectations and their professional responsibilities when using technology.

This AUP will help Elms School ensure that all visitors understand the school expectations regarding safe and responsible technology use.

Policy scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services provided to me or accessed as part of my role within Elms 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 systems and communication technologies**.**

2. I understand that Elms School AUP should be read and followed in line with the school staff code of conduct.

3. I am aware that this AUP does not provide an exhaustive list; visitors and volunteers should ensure that all 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.

Data and image use

4. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including GDPR.

5. I understand that I am not allowed to take images or videos of students.

Classroom practice

6. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of students.

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

8. I will support staff in reinforcing safe behaviour whenever technology is used on site and I will promote online safety with the students in my care.

9. I will immediately report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the Designated Safeguarding Lead (DSL) in line with the school child protection and online safety policy.

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

Use of mobile devices and smart technology

11. In line with the school mobile and smart technology policy, I understand that **mobile devices and smart technology e.g. mobile phones and personal devices are not permitted.**

Online communication, including the use of social media

12. I will ensure that my online reputation and use of technology and is compatible with my role within the school. This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.
    - I will take appropriate steps to protect myself online as outlined in the child protection and online safety/social media policy
    - I will not discuss or share data or information relating to students, staff, school business or parents/carers on social media.
    - I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with the school code of conduct and the law.

13. My electronic communications with students, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
    - All communication will take place via school approved communication channels such as via a school provided email address, account or telephone number.
    - Communication will not take place via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
    - Any pre-existing relationships or situations that may compromise my ability to comply with this will be discussed with the DSL and/or headteacher.

Policy compliance, breaches or concerns

14. If I have any queries or questions regarding safe and professional practice online either in school or off site, I will raise them with the Designated Safeguarding Lead and/or the headteacher.

15. 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.

16. 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.

17. 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.

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

19. I will report and record concerns about the welfare, safety or behaviour of students or parents/carers online to the Designated Safeguarding Lead in line with the school child protection policy.

20. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with the allegations against staff policy.

21. I understand that if the school believes that unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school may invoke its disciplinary procedures.

22. 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 Elms School visitor/volunteer Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of visitor/volunteer: ……………………………………………………………………..……………

Signed: ………………………...

Date

(DDMMYY)……………………………………………...

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the school boundaries and requirements when using the school Wi-Fi systems and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list, and all members of the school community are reminded that technology use should be consistent with our ethos, other appropriate policies, and the law.

1. The school provides Wi-Fi for the school community and allows access for **education use.**

2. I am aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The school takes no responsibility for the security, safety, theft, insurance, and ownership of any device used within the school premises that is not the property of the school.

3. The use of technology falls under Elms School Acceptable Use of Technology Policy (AUP), online safety policy and behaviour policy which all students /staff/visitors and volunteers must agree to and comply with.

4. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

5. School owned information systems, including Wi-Fi, must be used lawfully; 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.

6. I will take all practical steps necessary to make sure that any equipment connected to the school service is adequately secure, such as up-to-date anti-virus software, systems updates.

7. The school wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.

8. The school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

9. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.

10. I will not attempt to bypass any of the school security and filtering systems or download any unauthorised software or applications.

11. My use of school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

12. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

13. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead as soon as possible.

14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead or the headteacher.

15. I understand that my use of the school Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agreed to comply with <school name> Wi-Fi Acceptable Use Policy.

Name ……………………………………………………………………………………………………..…...

Signed: ………………………..

Date (DDMMYY)……………………..

Acceptable Use Policy (AUP) for Remote Learning

KCSIE states "*Schools and colleges are likely to be in regular contact with parents and carers. Those communications should be used to reinforce the importance of children being safe online and parents and carers are likely to find it helpful to understand what systems schools and colleges use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online".*

Additional information and guides on specific platforms can be found at:

- https://coronavirus.lgfl.net/safeguarding
- https://swgfl.org.uk/resources/safe-remote-learning/video-conferencing-for-kids-safeguarding-and-privacy-overview/

Further information and guidance for SLT and DSLs regarding remote learning:

- Local guidance:
  - Kelsi:
    - Online Safety Guidance for the Full Opening of Schools
  - The Education People: Covid-19 Specific Safeguarding Guidance and Resources
    - 'Safer remote learning during Covid-19: Information for School Leaders and DSLs'
- National guidance:
  - DfE: 'Safeguarding and remote education during coronavirus (COVID-19)
  - SWGfL: Safer Remote Learning
  - LGfL: Coronavirus Safeguarding Guidance
  - NSPCC: Undertaking remote teaching safely
  - Safer Recruitment Consortium: Guidance for safer working practice

Remote Learning AUP - Staff Statements

Elms School Staff Remote Learning AUP

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

Leadership oversight and approval

1. Remote learning will only take place using **school systems**.
   - **Microsoft Teams** has been assessed and approved by **the headteacher.**

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

3. Online contact with students **and/or** parents/carers will not take place outside of the operating times of the school day.
4. All remote lessons will be formally timetabled; **a member of SLT, DSL and/or head of department** is able to drop in at any time.

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 **Microsoft Teams** 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. All participants will be made aware that **Microsoft Teams** records activity.

9. 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.

10. Only members of the Elms School community will be given access to **Microsoft Teams**.

Session management

11. Staff will record the length, time, date, and attendance of any sessions held.

12. Appropriate privacy and safety settings will be used to manage access and interactions.

13. When live streaming with students:
    - contact will be made via students **school** provided email accounts **and/or** logins.
    - staff will **mute/disable** students' videos and microphones
    - at least 2 members of staff will be present.
        - If this is not possible, SLT approval will be sought.

14. Live 1:1 sessions will only take place with approval from the **headteacher.**

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.
    - Students **and/or** parents/carers should not forward or share access links.
    - If students or parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
    - Students 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.

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.

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:
    - **Students, reporting concerns to the member of staff running the session or telling 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 the **Head of School**.

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 **restricting/removing use, contacting police if a criminal offence has been committed.**

26. Any safeguarding concerns will be reported to Designated Safeguarding Lead, in line with our child protection policy.

I have read and understood the <school name> Acceptable Use Policy (AUP) for remote/online learning.

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

Date………………………………………………………………………………………

Remote Learning AUP – Student Statements

Elms School Student Remote Learning AUP

1. I understand that:
   - these expectations are in place to help keep me safe when I am learning at home using **Microsoft Teams**.
   - I should read and talk about these rules with my parents/carers.
   - remote/online learning will only take place using **Microsoft Teams** and during usual **school** times.
   - my use of **Microsoft Teams** is monitored to help keep me safe.

2. Only members of the Elms School community can access **Microsoft Teams**.
   - I will only use my **school** provided email accounts **and/or** login to access remote learning.
   - I will use privacy settings as **agreed with my teacher/set up the school.**
   - I will not share my login/password with others.
   - I will not share any access links to remote learning sessions with others.

3. When taking part in remote learning I will behave as I would in the classroom.

4. When taking part in live sessions I will:
   - mute my video and microphone.
   - wear appropriate clothing and be in a suitable location.
   - ensure backgrounds of videos are neutral and personal information/content is not visible.
   - use appropriate alternative backgrounds.
   - attend the session in full. If for any reason I cannot attend a session in full, I will let my teacher know.
   - attend lessons in a shared/communal space or room with an open door and/or where possible when I can be supervised by a parent/carer or another appropriate adult.

5. If I am concerned about anything that takes place during remote learning, I will:
   - **report concerns to the member of staff running the session or tell a parent/carer.**

6. I understand that inappropriate online behaviour or concerns about my or others safety during remote/online learning will be taken seriously. This could include:
   - **restricting/removing access, informing parents/carers, contacting police if a criminal offence has been committed.**

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

Name………………………………………………. Signed……………………………..………………….

Class…………………………………...…………. Date……………………………………………….……….

Parent/Carer’s Name……………………………...…………………………....…. (*If appropriate*)

Parent/Carer’s Signature………………………………………….………………… (*If appropriate*)

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