Acceptable Use of Technology Policy 2023-24

Approved by: Awaiting ratification	**Date:**
Last reviewed on:	
Next review due by:	

Version 1

Published August 2023

Contents

Acceptable Use of Technology Policy 2023-24 1
Contents 2
Child/Pupil/Student Acceptable Use of Technology 4
Early Years and Key Stage 1 (0-6) 4
Key Stage 2 (7-11) 4
Children with Special Educational Needs and Disabilities (SEND) 6
Acceptable Use of Technology for Parents/Carers 8
Acceptable Use of Technology for Staff, Visitors and Volunteers 10
Wi-Fi Acceptable Use Policy 15
Acceptable Use Policy (AUP) for Remote/Online Learning 17
Remote/Online Learning AUP - Staff 17
Remote/Online Learning AUP Template – Pupil/Student Statements 20

DEALT recommends that DSLs and leaders access the following national guidance and/or seek advice from the Education Safeguarding Service.

- Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - DfE Guidance - GOV.UK (www.gov.uk)
- Appropriate Filtering and Monitoring Guidance - UK Safer Internet Centre
- Filtering and monitoring - Questions for governors, proprietors and trustees - UK Safer Internet Centre
- Filtering and Monitoring Webinars - SWGfL

Disclaimer

Kent County Council make every effort to ensure that the information in this document is accurate and up to date. If errors are brought to our attention, we will correct them as soon as practicable. The copyright of these materials is held by Kent County Council. However, educational settings that work with children and young people are granted permission to use all or part of the materials for not-for-profit use, providing Kent County Council copyright is acknowledged and we are informed of its use.

Child Acceptable Use of Technology

Early Years and Key Stage 1 (0-6)

- I understand that the DEALT's 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 online links and buttons when I know what they do. If I am not sure, I ask an adult first.
- I keep my personal information and passwords safe.
- I only send messages online which are polite and friendly.
- I know the staff at my school can see what I am doing online when I use school and including if I use them at home for school user account such as Purple Mash.
- I always tell an adult, teacher or 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 School rules:
    - The school behaviour policy will be followed.
- I have read and talked about these rules with my parents/carers.

Shortened KS1 version (for use on posters or with very young children)

- 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.

Key Stage 2 (7-11)

I understand that the DEALT 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 will not use my own personal device, laptop, tablet, mobile phone, or smart products in school**.**
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher or school has chosen.
- 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.

Tell

- If I see anything online that I should not or if I see something online that makes me feel worried or upset, I will minimise the screen, shut the laptop lid, turn off the screen and tell an adult immediately.
- If I am aware of anyone being unsafe with technology, I will report it to a teacher/adult at school.
- I know it is not my fault if I see, or someone sends me, something upsetting or unkind 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.

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 owned devices and networks are monitored to help keep me safe, including if I use them at home. This means someone at the school may be able to see and/or check my online activity when I use school devices and/or networks if they are concerned about my or anyone else's safety or behaviour.
- If, for any reason, I need to bring a personal device, for example a smart/mobile phone and/or other wearable technology into school I know that it is to be handed in to the office and then collected at the end of the school day.
- 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 or to see help..
- I know that if I do not follow the school rules then:
    - The school behaviour policy will be followed.

Shortened KS2 version (for use on posters)

- I ask a teacher/adult about which websites I can use.
- I will not assume information online is true.
- I know there are laws that stop me copying online content.
- I know I must only open online messages that are safe. If I am unsure, I will not open it without speaking to an adult first.
- I know that people online are strangers, and they may not always be who they say they are.
- If someone online suggests meeting up, I will always talk to an adult straight away.
- I will not use technology to be unkind to people.
- I will keep information about me and my passwords private.
- I always talk to an adult if I see something which makes me feel worried.
- I know my use of school devices and systems can be monitored.

Children/Pupils/Students with Special Educational Needs and Disabilities (SEND)

Learners with SEND functioning at Levels P4 –P7

- 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:
    - The school behaviour policy will be followed in line with my understanding.

Learners with SEND functioning at Levels P7-L1 (Based on Childnet's SMART Rules)

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:
    - The school behaviour policy will be followed in line with my understanding.

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.

Pupil Acceptable Use Policy Agreement Form

My School's Acceptable Use of Technology Policy – Child Agreement

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

I agree to follow the AUP when:

1. I use school devices and systems, both on site and at home.
2. I use my own equipment out of the school, including communicating with other members of the school or when accessing school systems.

Name……. Signed…….……..….

Class…….…… Date…….

Parent/Carer's Name……...…….....

Parent/Carer's Signature…….…….

Date……

Acceptable Use of Technology for Parents/Carers

Parent/Carer AUP Acknowledgement Form

DEALT Acceptable Use of Technology Policy Acknowledgment

1. I have read and discussed DEALT's child 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 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 child, could have repercussions for the orderly running of the school, if a child is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school/setting.

3. I understand that any use of school devices and systems are appropriately filtered; this means we have systems in place that report weekly to the school online activity. This report is looked at by the Designated Safeguarding Lead and Headteacher. All staff follow our monitoring and filtering policy. Any concerns from this are reported and dealt with immediately.

4. I am aware that my child's use of school provided devices and systems will be monitored for safety and security reasons, when used on and offsite. Monitoring approaches are in place 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.

5. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems as above, to ensure my child is safe when they use school devices and systems, on and offsite. I however understand that the school cannot ultimately be held responsible for filtering breaches that occur due to the dynamic nature of materials accessed online, or if my child is using a personal device, including mobile or smart technologies.

6. I am aware that the school mobile and smart technology policy states that my child cannot use personal devices, including mobile and smart technology on site.

7. I understand that my child needs a safe and appropriate place to access remote/online learning, for example, if the school is closed. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. I understand my role and responsibility in supporting the school 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

Staff Acceptable Use of Technology Policy (AUP)

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use a DEALT School'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 children, 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 DEALT'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 Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the school or accessed by me as part of my role within a DEALT School professionally and personally, both on and offsite. This may include my use of devices such as laptops, mobile phones, tablets, digital cameras, as well as IT systems and networks, email. data and data storage, remote learning systems and communication technologies**.**

2. I understand that DEALT's 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.

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 children.

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/online learning, I will comply with the school remote/online 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.
    - 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. Leaders should include any specific requirements, for example, how often passwords should be changed etc.
    - I will protect the devices in my care from unapproved access or theft.

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 Headteacher.

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

11. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including UK 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.

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

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 Headteacher as soon as possible.

17. If I have lost any school related documents or files, I will report this to the Headteacher as soon as possible.

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

Classroom practice

19. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by DEALT as detailed in the Child Protection Policy, and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training. **Leaders should ensure the online safety or child protection policy includes specific details for staff relating to regarding expectations, applicable roles and responsibilities for appropriate filtering and monitoring.**

20. If there is failure in the filtering software or abuse of the filtering or monitoring systems, for example, I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL/Headteacher in line with the school child protection policy.

21. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces.

22. I will promote online safety with the children 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 children 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 children who may be impacted by the content.
    - Informing the DSL and/or leadership team if I am teaching topics which could create unusual activity on the filtering logs, or if I believe the filtering system is placing unreasonable restrictions on teaching, learning or administration.
    - make informed decisions to ensure any online safety resources used with children is appropriate.

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 have read and understood the school mobile and smart technology and social media policies which addresses use by children and staff.

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 policy, staff code of conduct, social media policy and the law.

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

28. My electronic communications with current and past children 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 children, 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 children and/or their parents/carers.
    - If I am approached online by a current or past children or parents/carers, I will not respond and will report the communication to the 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 children or parents/carers online to the DSL in line with DEALT's 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 devices information systems to monitor policy compliance and to ensure the safety of children and staff. This includes monitoring all school provided devices and school systems and networks including school provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school provided devices, systems and/or networks. 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 devices, systems or networks 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 DEALT 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)……

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 the education at school.

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 DEALT's Acceptable Use of Technology Policy (AUP), online safety policy and behaviour policy as data security, child protection, online safety policies which all children /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 DEALT Wi-Fi Acceptable Use Policy.

Name ……..…...

Signed: …….....Date (DDMMYY)……...

Acceptable Use Policy (AUP) for Remote/Online Learning

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

- LGfL: Safeguarding Considerations for Remote Learning
- SWGfL: Which Video Conference platform is best?

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
  - NSPCC: Undertaking remote teaching safely
  - Safer Recruitment Consortium: Guidance for safer working practice

Remote/Online Learning AUP Template - Staff Statements

DEALT Staff Remote/Online Learning AUP

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

Leadership oversight and approval

1. Remote/online learning will only take place using Purple Mash or Office 365 TEAMS.
   - Purple Mash and Office 365 TEAMs has been assessed and approved by the headteacher.

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

3. Online contact with children **and/or** parents/carers will not take place outside of the operating times as defined by the Headteacher:
    - 8.00 – 6.00pm (8.45-3.15 learning time)

4. All remote/online lessons will be formally timetabled**;** The Headteacher is able to drop in at any time.

5. Live-streamed remote/online learning sessions will only be held with approval and agreement from the headteacher.

Data Protection and Security

6. Any personal data used by staff and captured by Office 365 TEAMS when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.

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

8. All participants will be made aware that Office 365 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 DEALT School community will be given access to Office 365 TEAMs.

11. Access to Office 365 TEAMS will be managed in line with current IT security expectations.

Session management

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

13. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:

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

15. Live 1:1 sessions are not permitted.

16. 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.
- Children **and/or** parents/carers should not forward or share access links.
- If children or parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
- Children 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.

17. Alternative approaches and/or access will be provided to those who do not have access.

Behaviour expectations

18. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.

19. 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.
    - Setting decisions about if other attendees can or cannot record events for their own use, and if so, any expectations or restrictions about onward sharing.

20. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.

21. 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.

22. 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

23. Participants are encouraged to report concerns during remote and/or live-streamed sessions to Headteacher/ DSL

24. 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 Headteacher/ DSL.

25. 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.

26. Sanctions for deliberate misuse may include, restricting/removing use, contacting police if a criminal offence has been committed.

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

I have read and understood the DEALT Acceptable Use Policy (AUP) for remote/online learning.

Staff Member Name: ……

Date……

Remote/Online Learning AUP Template – Pupil/Student Statements

DEALT's Pupil Remote/Online Learning AUP

1. I understand that:
    - these expectations are in place to help keep me safe when I am learning at home using system name, for example Microsoft Teams etc.
    - 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 DEALT Schools community can access our system.
    - 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.
    - 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/online learning I will behave as I would in the classroom. This includes**:**
    - Using appropriate language.
    - Not taking or recording images/content without agreement from the teacher and/or those featured.

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/online learning, I will:
    - Tell the teacher or my parents/carers

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 DEALT's Pupil Acceptable Use Policy (AUP) for remote learning.

Name…… Signed……

Class……..…… Date……

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

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

Date……

DEALT