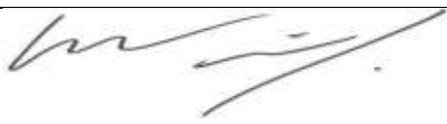




**Online Safety Acceptable Use Policies**  
**December 2020**

Policy lead	Kayleigh Simpson and Matt Rawling
Date approved by Governing Body	December 2020
Governor signature	
Review date	December 2021

## Acceptable Use of Technology for Families

*As a school, we are keen to promote safe technology use both in and out of school. As such, the children have devised their own 'rules' to follow which they have agreed and are attached to this document. As a school, we feel that modelling safe technology use and talking about safe behaviours is fundamental in ensuring that your child has the best possible chance of being safe online and reporting concerns appropriately if they do occur. In school we offer regular e-safety lessons following the project Evolve framework (this can be found online). We have some statements, documented below, which we feel are important for parents to understand and follow to support their child and the school. If you do not agree with any of the statements below, please contact a Designated Safeguarding Lead (Kayleigh Simpson, Matt Rawling or Hannah Ferris)*

1. I, with my child, have read and discussed Repton Manor Primary School learner acceptable use of technology policy (AUP) and understand that the AUP will help keep my child safe online.
2. I understand that the AUP applies to my child use of school devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns.
3. I am aware that any use of school devices and systems may be monitored for safety and security reason to keep my child safe and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
4. I am aware that the school mobile technology policy states that my child cannot use personal device and mobile technology on site.
5. I understand that my child needs a safe and appropriate place to access remote learning if school is closed in response to Covid-19. I will ensure my child's access to remote learning is appropriately supervised. When accessing video learning, I will ensure they are an appropriate location and that they are suitably dressed.
6. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use school devices and systems. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet or if my child is using mobile technologies.
7. I with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.
8. I understand that the school will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety.
9. I will inform the school or other relevant organisations if I have concerns over my child's or other members of the school communities' safety online.
10. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
11. I will support the school online safety approaches. I will use appropriate parental controls and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

# Acceptable Use of Technology for Staff

## Staff Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Repton Manor Primary School IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for learners, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

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

### Policy Scope

1. I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within Repton Manor Primary School both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning and online and offline communication technologies.
2. I understand that Repton Manor Primary School's 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.
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 educational use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed.
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.
- I will use a 'strong' password to access school systems and will not disclose my password or security information to others..
  - I will protect the devices in my care from unapproved access or theft.
8. 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 technician.
9. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.
10. 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. ***Please speak to the IT technician if you need support with this.***
11. 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.
12. 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.
13. 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.
14. I will not attempt to bypass any filtering and/or security systems put in place by the school.
15. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the IT technician (Simon Rogers) as soon as possible.

16. If I have lost any school related documents or files, I will report this to the IT Technician (Simon Rogers) and school Data Protection Officer (Vikki Reeves) as soon as possible.

17. I understand images of learners must always be appropriate and should only be taken with school provided equipment and taken/published where learners and their parent/carer have given explicit consent.

## **Classroom Practice**

18. 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.

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

20. I will promote online safety with the learners in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:

- exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
- creating a safe environment where learners feel comfortable to 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) (Kayleigh Simpson or Matt Rawling) or a deputy (Hannah Ferris) as part of planning online safety lessons or activities to ensure support is in place for any learners who may be impacted by the content.
- make informed decisions to ensure any online safety resources used with learners is appropriate.

21. 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.

22. 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.

## **Use of Social Media and Mobile Technology**

23. I have read and understood the school policy which covers expectations regarding staff use of mobile technology and social media.

24. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role and in line with the staff behaviour policy/code of conduct, when using school and personal systems. This includes my use of email, text, social media and any other personal devices or mobile technology.

- I will take appropriate steps to protect myself online when using social media as outlined in the social media policy.
- I am aware of the school expectations with regards to use of personal devices and mobile technology, including mobile phones as outlined in the mobile technology policy.
- I will not discuss or share data or information relating to learners, staff, school business or parents/carers on social media.
- I will ensure that my use of technology and the internet does not undermine my professional role or interfere with my work duties and is in accordance with the school behaviour policy/code of conduct and the law.

25. My electronic communications with current and past learners and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.

- I will ensure that all electronic communications take place in a professional manner via school approved and/or provided communication channels and systems, such as a school email address, user account or telephone number.
- I will not share any personal contact information or details with learners, such as my personal email address or phone number.
- I will not add or accept friend requests or communications on personal social media with current or past learners and/or parents/carers.
- If I am approached online by a learner or parents/carer, I will not respond and will report the communication to one of the schools DSL's or Deputy DSL's (Matt Rawling, Kayleigh Simpson and Hannah Ferris)
- Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the DSL and/or Head Teacher.

26. 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.

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.

## **Policy Compliance**

30. I understand that the school may exercise its right to monitor the use of 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.

## **Policy Breaches or Concerns**

31. 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.

32. I will report concerns about the welfare, safety, or behaviour of staff to the Head Teacher, in line with the allegations against staff policy.

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

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

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

**I have read, understood and agreed to comply with Repton Manor Primary 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 and Volunteer Acceptable Use of Technology Policy

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

This AUP will help Repton Manor Primary School ensure that all visitors and volunteers understand the schools 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 Repton Manor Primary School both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning systems and communication technologies.
2. 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

3. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including GDPR.
4. I understand that I am not allowed to take images or videos of learners unless on a school device with the class teachers approval.

## Classroom Practice

5. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of learners.
6. I will support staff in reinforcing safe behaviour whenever technology is used on site and I will promote online safety with the children in my care.
7. I will immediately report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the Designated Safeguarding Lead (DSL) (Kayleigh Simpson, Matt Rawling or Deputy DSL Hannah Ferris) in line with the school child protection policy.
8. 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 Social Media and Mobile Technology

9. 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.
  - I will not discuss or share data or information relating to learners, 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/behaviour policy and the law.
10. Any communication with parents/carers, children and professionals will be face to face and will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
- 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 this will be discussed with the DSL (Kayleigh Simpson or Matt Rawling) and/or Head Teacher.
11. 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 Designated Safeguarding Lead (Kayleigh Simpson/Matt Rawling/Hannah Ferris) and/or the Head Teacher.
12. 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.
13. 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.
14. 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.

## **Policy Compliance, Breaches or Concerns**

15. 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, to monitor policy compliance and to ensure the safety of learners, staff and visitors/volunteers. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
16. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the Designated Safeguarding Lead (Kayleigh Simpson/Matt Rawling/Hannah Ferris) in line with the school child protection policy.
17. I will report concerns about the welfare, safety, or behaviour of staff to the Head Teacher, in line with the allegations against staff policy.

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

19. 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 Repton Manor Primary 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).....

# Repton Manor Primary School Staff Remote Learning AUP

The Remote Learning Acceptable Use Policy (AUP) is in place to safeguarding all members of the 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 Microsoft Teams, Zoom or Google Classrooms
  - These systems have been assessed and approved by the ICT technician and Head Teacher.
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 Kayleigh Simpson or Matt Rawling, 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 learners and/or parents/carers will not take place outside of the operating times as defined by SLT without prior consent:
  - Monday to Friday between 08:00 and 17:00
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 Senior Leadership Team.

## Data Protection and Security

6. Any personal data used by staff and captured by the online learning platforms 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 and will not be shared unless necessary and with the appropriate person.
8. All participants will be made aware that online platforms can records activity if the content is being recorded. Only needed if the session is recorded by the system: settings should amend as appropriate to the approach and system being used. Please note, consent from those involved in the session is required if settings are recording activity. Settings should be clear about how recordings will be stored, how long they will be kept for and who will have access to them, in line with your existing data protection policy.
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 Repton Manor Primary School community will be given access to the online learning platform login details and passwords.
11. Access to the online learning system will be managed in line with current IT security expectations. E.g the use of strong passwords, not sharing passwords, logging off when not in use, locking screen when not with the device. as outlined in policy name.

## Session Management

12. Staff will record the length, time, date, and attendance of any sessions held. This will be recorded on sheets disseminated by the DSL in the event of a lockdown.
13. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
  - Not allowing children to share screens, staff being aware of how to mute children, keeping meeting ID's private, disabling chat where appropriate.
14. When live streaming with learners:
  - contact will be made via learners' school provided email accounts or logins
  - staff will mute/disable learners' videos and microphones as appropriate in line with the session being taught and age of the children.
  - at least 2 members of staff will be present. Amend as appropriate to system and SLT decision.
    - If this is not possible, SLT approval will be sought.
15. Live 1 to 1 sessions will only take place with approval from a member of SLT.
16. A pre-agreed invitation/email (as relevant to system being used) detailing the session expectations will be sent to those invited to attend.
  - Access links should not be made public or shared by participants. If relevant to system being used.
  - 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. Amend as appropriate.
  - 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.
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, but is not limited to;
  - Appropriate language will be used by all attendees.
  - Staff will not take or record images for their own personal use.
  - Recordings of learning should not be sent without the knowledge of Senior Leadership Team
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.
  - Ensure that family are not visible in the background
  - Behave professionally and model safe internet behaviour.
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:
- Insert specifics or reference where to find them. For learners, schools could insert age/ability appropriate details e.g. reporting concerns to the member of staff running the session, telling a parent/carer etc.
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 Kayleigh Simpson DSL/PSM.
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 of online learning, contacting parents or contacting police if a criminal offence has been committed.
27. Any safeguarding concerns will be reported to Kayleigh Simpson, Matt Rawling or Hannah Ferris, Designated Safeguarding Lead, in line with our child protection policy.

**I have read and understood the Repton Manor Primary School Acceptable Use Policy (AUP) for remote learning.**

Staff Member Name: .....

Date.....