Lydden and River Primary Schools Federation

Acceptable Use of Technology Policy

Key Details

Designated Safeguarding Lead (s):

Mrs V Alliston- River Primary School, Acting Headteacher.

Mrs C Lintott – Lydden Primary School, Acting Headteacher

Named Governor with lead responsibility: Dr K Grilli

Date written/updated: September 2024

Date agreed and ratified by Governing Body : October 2024

Date of next review: September 2025

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 Lydden and River Federation 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 Lydden and River Federation 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 Lydden and River Federation, 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 the Lydden and River Federation 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 Lydden and River Federation 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. 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 not

allowed. Internet services should not be accessed for entertainment, including personal social media accounts. However, the federation allows access to check personal emails and appointments (including Doctors, MOT, Building services).

5. Where I deliver or support remote/online learning, I will comply with the school remote/online learning AUP.

Data and system security

6. 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. *For example, not leaving devices visible or unsupervised in public places.*

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

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 technician.

10. 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.
    - Any data being shared online, such as via cloud systems or artificial intelligence tools (AI), will be suitably risk assessed and approved by the school, Data Protection Officer and leadership team prior to use to ensure it is safe and legal. Only approved education AI support should be used.

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 in a password protected environment or school approved VPN.

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 ICT technician, Sarah Higgins or ICT Support Provider (SNS - Peter Baron) as soon as possible.

16. If I have lost any school related documents or files, I will report this to the ICT technician, Sarah Higgins or ICT Support Provider (SNS - Peter Baron) and school Data Protection Officer (Accordio Ltd) as soon as possible.

17. Any images or videos of children will only be used as stated in the school camera and image use policy (Safeguarding file on Sharepoint). 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

18. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by Lydden and River Federation as detailed in the Safeguarding and Online Safety policies and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training.

19. 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 and IT staff (Miss S Higgins), in line with the school child protection/online safety policy.

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 safeguarding and child protection, online safety and the remote learning AUP.

21. I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our school community. However, I also recognise that AI tools can also pose risks, including, but not limited to, bullying and harassment, abuse and exploitation (including child sexual abuse), privacy and data protection risks, plagiarism and cheating, and inaccurate, harmful and/or biased material. Additionally, its use can pose moral, ethical and legal concerns

if not carefully managed. As such, I understand that the use of AI as part of our education/curriculum approaches is permitted by staff only.

- A risk assessment will be undertaken, and written approval will be sought from the senior leadership team prior to any use of AI tools (for example if used in the classroom, or to support lesson planning or assessments).
- Any misuse of AI will be responded to in line with relevant school policies, including but not limited to, anti-bullying, staff code of conduct and child protection.

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) (River – Mrs V Alliston, Lydden – Mrs C Lintott or a deputies (Mrs J Brown, Mrs t Moody, Miss L Chase) 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 and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, misuse, plagiarise, or distribute 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, 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 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 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 Acting 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 the school child protection policy.

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

39. **I have read, understood and agreed to comply with Lydden and River Primary Schools Federation 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 education use only.

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 Lydden and River Federation Acceptable Use of Technology Policy (AUP), online safety policy, behaviour policy and child protection. 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 (River – Mrs V Alliston, Lydden Mrs C Lintott) as soon as possible.

14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead (River – Mrs V Alliston, Lydden Mrs C Lintott) or the Acting 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 Lydden and River Federation Wi-Fi Acceptable Use Policy.

Name ……..…...

Signed: …….....Date (DDMMYY)……..n

Template Acceptable Use Policy (AUP) for Remote/Online Learning

Remote/Online Learning AUP - Staff Statements

Lydden and River Federation Staff Remote Learning AUP

The Remote/Online Learning Acceptable Use Policy (AUP) is in place to safeguarding all members of our 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 Microsoft 365 and Teams.

- This has been assessed and approved by the headteacher or a member of Senior Leadership Team (SLT).

2. Staff will only use school managed or specific, 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 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 SLT: 8am – 4pm (this allows for any email contact)

4. All remote/online lessons will be formally timetabled**;** a member of SLT and/or DSL 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 Acting headteacher or a member of SLT.

Data Protection and Security

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

7. All participants will be made aware that Teams/Microsoft 365 records activity if initiated by the class teacher. All would be notified, if this was the case and children would be instructed to keep their cameras off.

8. Staff will not record lessons or meetings using personal equipment.

9. Only members of the Lydden and River Federation community will be given access to Microsoft 365.

10. Access to Microsoft 365 will be managed in line with current IT security expectations as outlined in our Staff Acceptable Use and Mobile Technologies policy.

Session management

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

12. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
    - language filters, disabling/limiting chat, staff not permitting children/young people to share screens, keeping meeting IDs private, use of waiting rooms/lobbies or equivalent.

13. When live streaming with children:
    - contact will be made via children's school provided email accounts or logins.
    - staff will mute children's videos and microphones. They will be allowed under staff control at specific times.
    - 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/a member of SLT. It is recommended a parent/carer is present in the room if possible (however, this may not be appropriate if providing counselling or safeguarding support).

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.
    - Children **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.

16. Alternative approaches or access will be provided to those who do not have access. E.g. through loaned devices.

Behaviour expectations

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

    - 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.
    - Attendees can or cannot record events for their own use or take screenshots to distribute.

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

19. 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.

20. 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

21. Participants are encouraged to report concerns during remote or live-streamed sessions:
- Reporting concerns to the member of staff running the session or telling a parent/carer.

22. 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 Acting Headteacher or a member of SLT.

23. 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.

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

25. Any safeguarding concerns will be reported to the Designated Safeguarding Lead (River – Mrs V Alliston, Lydden – Mrs C Lintott), in line with our child protection policy.

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

Staff Member Name: ……

their professional responsibilities when using technology. This AUP will help Lydden and River Federation ensure that all visitors and volunteers 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, either provided to me by the school or accessed by me as part of my role within Lydden and River Federation professionally and personally. 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 Lydden and River Federation 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.

4. 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.

5. 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.

6. 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.

Data and image use

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

8. I understand that I am not allowed to take images or videos of children. Any images or videos of children will only be taken if directed to do so by the class teacher or teaching assistant, in line with the school camera and image use policy.

Classroom practice

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

10. I will support and reinforce safe behaviour whenever technology is used on site, and I will promote online safety with the children in my care.

11. If I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material by any member of the school community, I will report this to the DSL and IT technician (Mrs S Higgins), in line with the school child protection and online safety policy.

12. I will respect copyright and intellectual property rights and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, misuse, plagiarise, or distribute them.

Use of mobile devices and smart technology

13. In line with the school mobile and smart technology policy, I understand that mobile phones and personal devices are not permitted to be used within the school, the only use of such devices may be in the staff room. Our social media and mobile technology policy details appropriate use.

Online communication, including the use of social media

14. 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, online safety and social media policy.
    - I will not discuss or share data or information relating to children, 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.

15. My electronic communications with children, 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 (River -Mrs V Alliston, Lydden – Mrs C Lintott)

Policy compliance, breaches or concerns

16. 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 (River -Mrs V Alliston, Lydden – Mrs C Lintott)

17. 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.

18. I will report and record concerns about the welfare, safety or behaviour of children or parents/carers online to the Designated Safeguarding Lead (River -Mrs V Alliston, Lydden – Mrs C Lintott) in line with the school child protection policy.

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

20. 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.

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

22. **I have read, understood and agreed to comply with Lydden and River Primary Schools Federation 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).....