Otford Primary School

Acceptable Use Policy

Date: March 2026

To be reviewed: March 2027

CONTENTS

Child Acceptable Use of Technology Statements

Although statements for children/pupils/students are collected within key stages, it is recommended that settings amend and adapt them according to their own cohorts needs.

Settings should ensure their AUP includes age and ability appropriate information and expectations relating to the specific use and monitoring of school provided devices and networks, services and/or systems, for example laptops, tablets and cloud computing, as well as use of learner owned devices such as mobile/smart phones, tablets and wearable technology.

The template statements and headers are suggestions only and some statements are duplicated; we encourage educational settings to work with their community to amend the statements so they can develop ownership and understanding of the expectations.

Early Years and Key Stage 1 (0-6)

- I understand that the school rules will help keep me safe and happy when I go online.
- I only go online when a grown-up is with me.
- I only click on online things online when I know what they do. If I am not sure, I ask a grown-up first.
- I keep my personal information and passwords safe.
- I only send polite and friendly messages online.
- I know the school can see what I am doing online when I use school computers/tablets and on Purple Mash if I use them at home.
- If I see something online that makes me feel upset, unhappy, or worried I will always tell a grown-up.
- I can visit www.ceopeducation.co.uk to learn more about keeping safe online.
- I know that if I do not follow the school rules: I may need to reflect and have time away from computers/tablets until I know how to be safe.
- I have read and talked about these rules with my parents/carers.

Key Stage 2 (7-11)

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

Safe

- I will be kind and respectful online, just like I am in school.
- I only send messages which are polite and friendly.
- I will only share pictures or videos online if they are safe, kind, and I have asked for permission first.
- I will only click on links if a trusted adult says they are safe.

- I know that people online might not be who they say they are. I will only chat with people I know or who a trusted adult says are safe.
- If someone online asks to meet me, I will tell a trusted adult straight away.

Learning

- I am not permitted to use my own personal smart devices and/or mobile phone at school.
- I always ask permission from an adult before using the internet.
- I only use websites, tools and/or search engines that my teacher has chosen or given me permission to use.
- I use school devices for school work unless I have permission otherwise.
- If I need to learn online at home, I will follow the same rules in this policy.

Trust

- I know that some things or people online might not be honest or truthful.
- If I'm not sure something online is true, I will check with other websites, books, or ask a trusted adult.
- I always credit the person or source that created any work, images, or text I use.
- I will use Artificial Intelligence (AI) tools safely and sensibly. I won't use them to cheat, copy other people's work, or say anything unkind. I know that AI tools can sometimes make mistakes. I will only use them when a teacher or trusted adult says it's okay.

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 makes me feel worried or upset, I will minimise the screen, shut the laptop lid, 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 something upsetting or unkind online.
- If I'm not sure about something online or it makes me feel worried or scared, I will talk to a trusted adult.
-

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 checked/monitored to help keep me safe, even 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 worried about my or anyone else's safety or behaviour.
- If, for any reason, I need to bring a personal device, like a smart/mobile phone and/or other wearable technology into school then I will hand it into the school office on arrival at school.
- I have read and talked about these rules with my parents/carers.
- I can visit www.ceopeducation.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: I may not be permitted to use school devices until I know and respect the safety rules.
-
- I will speak to an adult I trust if something happens to either myself or another student which makes me feel worried, scared, or uncomfortable.
- I will visit www.ceopeducation.co.uk, www.childnet.com and www.childline.org.uk to find out more about keeping safe online.
- I have read and talked about these expectations with my parents/carers.

Report

- I know that people online are not always who they say they are and that I must always talk to an adult before meeting any online contacts.
- If anything happens online which makes me feel worried or uncomfortable then I will speak to an adult I trust and visit www.ceopeducation.co.uk.

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 Otford 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 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 Otford 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 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 Otford Primary 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 Otford Primary School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school child protection policy.

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, for work purposes.

5. I understand that any equipment and internet services provided by my workplace is intended for education purposes and/or professional use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed.

6. Where I deliver or support remote/online learning, I will comply with this policy.

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.
    - I will protect the devices in my care from unapproved access or theft by keeping them safe and not unattended e.g. in vehicles

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

9. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT system manager.

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

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

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 provided 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 ICT Support Provider (EIS) as soon as possible.

17. If I have lost any school related documents or files, I will report this to the Headteacher and school Data Protection Officer 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 Otford Primary School 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.

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 and IT provider, 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 as listed in the AUP.

22. 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:
    - AI tools are only to be used responsibly and ethically, and in line with our school child protection expectation and AI policy
    - I am required to critically evaluate any AI-generated content for accuracy, bias, and appropriateness before sharing or using it in educational contexts.
    - AI must not be used to replace professional judgement, especially in safeguarding, assessment, or decision-making involving children.
    - Only approved AI platforms may be used with children. Children must be supervised when using AI tools, and I must ensure age-appropriate use and understanding prior to use.
    - Any misuse of AI will be responded to in line with relevant school policies.

23. 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.

24. 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

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, code of conduct and the law.

27. As outlined in the staff code of conduct:
    - 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 child/ren or parents/carers, I will not respond and will report the communication to the Headteacher 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 the school child protection policy.

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

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

3 **I have read, understood and agreed to comply with Otford 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 safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of our behaviour expectations and their professional responsibilities when using technology. This AUP will help Otford 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, either provided to me by the school or accessed by me as part of my role within Otford Primary School, 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 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.

3. 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.

4. 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.

5. 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

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

7. I understand that I am not allowed to take images or videos of children. Any images or videos of children will only be taken on school devices.

Classroom practice

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

9. 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.

10. 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 provider, in line with the school child protection policy.

11. 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

12. In line with the school mobile and smart technology policy, I understand that mobile phones and personal devices are only permitted to be used in the Staff only areas e.g. office/Staff room

Online communication, including the use of social media

13. 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 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/behaviour policy and the law.

14. 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 and headteacher.

Policy compliance, breaches or concerns

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

16. 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.

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

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

19. 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.

20. 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 Otford 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)…….....

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 Otford Primary School Acceptable Use of Technology Policy (AUP), online safety policy and behaviour policy 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 Otford Primary School Wi-Fi Acceptable Use Policy.

Name ……..…...

Signed: …….....Date (DDMMYY)……...