

Offham Primary School



Acceptable Use of Technology Policy Staff, Visitors and Volunteers

(Kent LADO Education Services 2025-2026 Template)

Date of Policy September 2026

Review Date July 2027

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Offham 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 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

- 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 Offham 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.
- I understand that Offham Primary School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school's Safeguarding Policy, Online Safety Policy and Staff Code of Conduct
- 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/setting devices and systems

- I will only use the equipment and internet services provided to me by the school for example school provided laptops, tablets 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/is allowed. This use at the school's discretion and can be revoked at any time.

Data and system security

- 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 schools systems.
- I will protect the devices in my care from unapproved access or theft.
- I will respect school system security and will not disclose my password or security information to others.
- I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the Headteacher and Lead DSL.
- I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.
- 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.
- All data must be saved on the shared online system, not on desktops or memory sticks/external hard drives.
- Artificial intelligence tools (AI) will be used in reference to 'The generative artificial intelligence (AI) in education policy paper'.

- 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.
- 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.
- I will not attempt to bypass any filtering and/or security systems put in place by the school.
- If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the Headteacher/Lead DSL.
- If I have lost any school related documents or files, I will report this to the Headteacher/Lead DSL who if required will report it to the Data Protection Officer.
- I understand images of children must always be appropriate and should only be taken with school provided equipment and only be taken/published where parent/carers have given explicit written consent.

Classroom practice

- I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by Offham Primary School as detailed in school policies, as discussed with me as part of my induction and/or ongoing safeguarding staff training.
- 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 Headteacher and Lead DSL.
- AI tools are only to be used responsibly and ethically, and in line with our school policies. AI must not be used to replace professional judgement, especially in safeguarding, assessment, or decision-making involving children.
- Any misuse of AI will be responded to in line with relevant school policies.

- 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.
 - 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.

- 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

- 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 Code of Conduct and the law.

- 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 Safeguarding Policy, Code of Conduct and the law.

- 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.

- I will not have any electronic communications with current and past children. Electronic communications with 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 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/past children.
- If I have links with parents in a friend capacity on social media/telephone devices all communications are on a personal basis and will not involve discussions around school.
- If I am approached online by a current or past children/pupils/students or parents/carers, I will not respond and will report the communication to my line manager and (name) 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

- 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.
- 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.
- 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.

- 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's Safeguarding Policy.
- I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher/Lead DSL.

Policy Compliance and Breaches

- 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 Lead DSL/Headteacher.
- 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.
- 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.
- 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.
- I understand that if the school/setting suspects criminal offences have occurred, the police will be informed.

Offham Primary School



Acceptable Use of Technology Policy Staff, Visitors and Volunteers

I have read and understood the acceptable use policy

Name:

Signature:

Date: