



Acceptable Use Policy for Employees, Governors, Volunteers & Visitors

September 2026

As a professional organisation with responsibility for safeguarding, all staff are expected to use technology in a professional, lawful, ethical and responsible manner.

This Staff Acceptable Use of Technology Policy (AUP) sets out Ospringe CE Primary School, expectations for safe technology use, professional conduct, safeguarding, data protection and system security. It is not intended to unduly limit appropriate teaching, learning or professional use of technology, but to help protect pupils, staff, systems and the wider school community from accidental or deliberate misuse.

All staff are asked to read, understand and sign this AUP.

Policy scope

1. I understand that this policy applies to my use of technology systems and services provided by the school or accessed by me as part of my role within Ospringe CE Primary both on and offsite. It also applies to personal use of technology where this is linked to my role, involves the Ospringe community, uses school systems or information, could affect safeguarding, professional boundaries, confidentiality or data protection, or could reasonably impact on my professional role or the reputation of the school.
2. I understand that Ospringe CE Primary School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school child protection policy and staff code of conduct.
3. I am aware that all staff should ensure that technology use is consistent with the school ethos, staff code of conduct and safeguarding policies, national and local education and child protection guidance, and the law.

Use of school devices and systems

4. I will use school -provided or approved equipment, systems and internet services when working with pupils, unless otherwise formally agreed by leaders.
5. I understand that school equipment, systems and internet services are provided for education and/or professional use. Reasonable personal use is permitted and, where allowed, must not interfere with my work duties, system security, safeguarding, confidentiality or professional boundaries. This permission is at the school's discretion and may be withdrawn at any time.

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 follow the [school's requirements for secure passwords, authentication and account access. I will keep authentication information secure and will not share passwords, verification codes or access credentials with others.
 - I will protect the devices in my care from unapproved access or theft. I will not leave devices visible or unsupervised in public places.
7. I will take care before opening links or attachments, including those apparently sent by a known contact. I will check unexpected or suspicious messages through an appropriate route and report suspected phishing or malicious content to Primary Technologies.
8. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from Primary Technologies.
9. I will ensure that any personal data is kept in accordance with data protection legislation, 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.
 - I will only process or share personal data through school approved systems and services and in line with the setting's data protection and information-security procedures. Any proposed new or changed use of cloud services, AI tools or other online systems involving personal data will be risk assessed and approved through the setting's agreed process before use. Where required, a Data Protection Impact Assessment will be completed.
10. 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.
11. 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.
12. 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.

13. I will not attempt to bypass any filtering and/or security systems put in place by the school.
14. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the Primary Technologies as soon as possible.
15. If I have lost any school related documents or files, I will report this to Primary Technologies, and the school Data Protection Officer (Angela Woodgate) as soon as possible.
16. I will follow the school image use policy when taking, using, storing or sharing images or recordings of pupils. Images and recordings must always be appropriate and must only be taken using school-provided or approved equipment. I will not use personal devices, including personal mobile phones, cameras, tablets, smart watches or other wearable technology, to take images or recordings of pupils. Images and recordings will only be taken, used or shared in line with the school image use policy, safeguarding expectations, data protection requirements and consent/lawful basis arrangements.

Classroom practice

17. I understand my role and responsibilities in relation to filtering and monitoring, as explained through induction, safeguarding training and relevant school policies.
18. If I become aware of a filtering or monitoring failure, or witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and Primary Technologies in line with the school child protection policy.
19. I will follow school expectations for safe technology use in classrooms, remote/online learning and other working spaces, including the use of approved platforms, search tools and AI tools.
20. I will follow the setting's agreed approach to screen use. Any use of screens, devices, apps or online content will be planned, purposeful, age appropriate and supervised, and will not replace face-to-face interaction, play, physical activity, rest, care routines or real-world exploration.
21. I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our school community. However, I 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, their use can pose moral, ethical and legal concerns if not carefully managed. As such, I understand that:
 - AI tools must only be used responsibly, ethically and where the tool, purpose and use have been approved by leaders. Any new, unapproved or changed use of AI tools will be risk assessed and approved before use, in line with child protection, data protection and professional conduct expectations.
 - I understand that AI-generated content must be checked for accuracy, bias, appropriateness, copyright and safeguarding implications before it is used or shared.

- I will not enter personal, sensitive, confidential, safeguarding, assessment or special category information, or images of pupils, staff or other identifiable individuals, into any AI tool unless the tool has been approved for that purpose, the use has been risk assessed, consent has been obtained where required, and the leadership team has confirmed that the processing is lawful and appropriate.
- I will not add or use AI note takers, transcription tools, recording bots or automated meeting summary tools in any meeting, lesson, supervision, training or professional discussion unless this has been agreed in advance by leadership. Where approved, I will ensure that participants are made aware and their use is transparent, proportionate and in line with safeguarding, confidentiality, consent, data protection and information governance expectations.
- I will not use AI to make decisions about pupils, families or staff, including decisions relating to safeguarding, behaviour, SEND, assessment, attendance, admissions, recruitment, allegations or pastoral support, without appropriate professional oversight and in line with setting policy.
- Only approved AI platforms may be used with pupils. Children must be supervised when using AI tools, and I must ensure age-appropriate use and understanding prior to use.
- I will report any concern involving AI misuse, including deepfake or manipulated content, impersonation, harmful AI-generated material, AI-facilitated bullying or harassment, or AI-generated nude/semi-nude imagery, in line with the school child protection, behaviour, anti-bullying, staff conduct and data protection procedures

22. 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 or being judged for talking about something which happened to them online.
- involving the DSL or a deputy as part of planning online safety lessons or activities to ensure support is in place for any pupils 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.
- making informed decisions to ensure any online safety resources used with pupils are 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 phones and smart devices

24. I will ensure that my use of mobile phones and smart devices is compatible with my professional role, does not interfere with my duties, and takes place in line with the staff code of conduct, mobile phone policy and the law.
25. I will model safe and professional use of mobile phones and smart devices and will support the school's expectations for children.
26. Where mobile phones or smart devices are used for professional purposes, such as authentication, learning activities, recording rewards or sanctions, or other agreed tasks, I will use school-provided devices where available. Where staff are permitted to use personal devices for professional purposes, this must be formally agreed by the school and managed in line with school policy.
27. Any use of a personal mobile phone or smart device for professional purposes, or in exceptional circumstances, must be transparent, necessary, proportionate and approved by the headteacher or other designated leader. Use must not compromise supervision, safeguarding, confidentiality, professional boundaries, data protection or the learning environment.

Online communication, including use of social media

28. I will ensure that my use of communication technology, including social media, is compatible with my professional role, does not interfere with my work duties, and takes place in line with the child protection policy, staff code of conduct, social media policy and the law.
29. I will protect myself, my professional reputation and the reputation of the school online. I will not discuss or share data or information relating to children, staff, school business or parents/carers on social media.
30. My electronic communications with current and former pupils 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-provided communication channels and systems, such as a school email address, user account or telephone number.
 - I will not use personal accounts, personal profiles, personal phone numbers, private messaging apps, gaming accounts or other personal communication channels to contact or communicate with pupils or their families, unless this has been formally approved, risk assessed and recorded by leaders.
 - I will not share any personal contact information or details with pupils, such as my personal address, email address or phone number.
 - I will not share personal information about my private life with pupils online, through messaging, social media, gaming platforms, apps or other digital communication channels. I will maintain appropriate professional boundaries in all digital communication.

- I will not add, follow, accept or respond to friend requests, direct messages or other personal online communication from current or former pupils, or their parents/carers, where this is linked to my role, the school, or could blur professional boundaries. Any attempted contact will be reported to my line manager and/or the DSL.
- Any pre-existing links, relationships or situations that affect how I apply the AUP or other relevant policies will be discussed with the DSL and/or Headteacher. This is to help safeguard pupils, staff and the wider school community by ensuring professional boundaries, safeguarding expectations and communication arrangements are clear.
- Where digital communication with pupils or families is required, I will follow the [school's expectations about when communication should take place, including any agreed arrangements for out-of-hours contact, emergency communication or role-specific responsibilities.

Policy concerns

31. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, terrorist material or adult pornography covered by the Obscene Publications Act.
32. I will not access, create, transmit, display, publish, forward, discuss, send, share or show any material or content that may be harmful, inappropriate, adult, offensive, unprofessional, or likely to harass, cause offence, inconvenience or needless anxiety to any other person. This applies when using school systems, school devices, personal devices, personal accounts, messaging apps, online platforms, social media or shared spaces. It includes content shared in staff rooms, offices, online groups or other staff communication spaces, where this takes place on school premises, during working time, or in any context linked to my role.
33. I will not engage in online or digital behaviour linked to my role that compromises safeguarding, professional boundaries, confidentiality, data protection, public confidence in my professional conduct or my ability to carry out my role.
34. I will report and record any concerns about the welfare, safety or behaviour of pupils or parents/carers online to the DSL in line with the school child protection policy.
35. I will report concerns about the welfare, safety, conduct, or behaviour of staff, including online, digital, device-related or technology-linked concerns, to the Headteacher, in line with the school child protection policy, staff code of conduct, low-level concerns procedures and/or allegations against staff policy.

Policy compliance and breaches

36. 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 DSL and/or the Headteacher.
37. I understand that the school may exercise its right to monitor the use of its devices and information systems to check policy compliance and help ensure the safety of pupils 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.
- Staff will be informed about the nature, purpose and extent of monitoring through this AUP, relevant policies, privacy information and/or staff guidance.

38. I understand that if the school believes 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].
39. If I find myself in a situation where my online contact, device use, recording, image use or AI use could be misinterpreted, I will report this promptly to the DSL/Headteacher so it can be recorded and managed transparently.
40. Any breach or concern involving online contact, device use, images, recordings, social media, AI use, confidentiality, data protection or professional boundaries must be reported to the Headteacher and/or DSL without delay, even if it appears minor, accidental or unlikely to meet the harm threshold.
41. I understand that if the school believes that unprofessional or inappropriate online or technology-related activity may have compromised safeguarding, professional boundaries, confidentiality, data protection, public confidence in professional conduct or my ability to carry out my role, the concern will be considered fairly, proportionately and confidentially, in line with relevant safeguarding, staff behaviour, low-level concerns, allegations, data protection and disciplinary procedures. Where the concern may meet the harm threshold, advice will be sought and/or a referral made to the Local Authority Designated Officer (LADO) in line with local allegations procedures. Where it does not meet this threshold, it will still be recorded and responded to appropriately.
42. Where a concern involves personal data, confidential information, safeguarding information, images, recordings, AI tools, transcription tools or unauthorised sharing, the DPO/data protection lead will be informed promptly so that any data protection, information governance or reporting requirements can be considered.
43. I understand that if the school suspects criminal offences have occurred, the police will be informed where appropriate.
44. I understand that this AUP cannot cover every possible situation. If I am unsure whether any use of technology, online communication, image use, recording, personal device use, social media, AI tool or digital contact is appropriate, I will seek advice from the DSL and/or Headteacher before taking action. I will act in a way that safeguards children, protects professional boundaries, and is open to scrutiny.