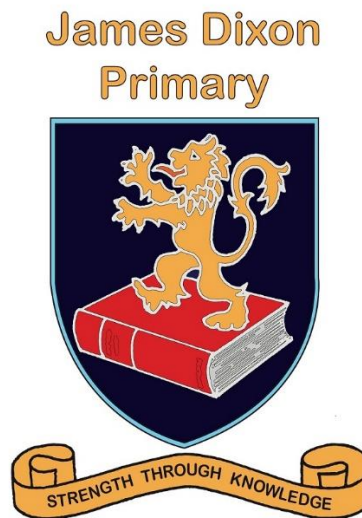


James Dixon Primary School



Acceptable Use of Technology for Staff, Visitors and Volunteers Agreement.

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

Our AUA 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 AUA will help ensure that all staff understand James Dixon Primary School's expectations regarding safe and responsible technology use, and can manage the potential risks posed. The AUA 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.

Scope

1. I understand that this AUA applies to my use of technology systems and services provided to me or accessed as part of my role within James Dixon Primary School both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras and email as well as IT networks, data and data storage and online and offline communication technologies.
2. I understand that James Dixon Primary School's Acceptable Use of Technology Agreement (AUA) should be read and followed in line with the staff code of conduct.
3. I am aware that this AUA does not provide an exhaustive list; all staff should ensure that technology use is consistent with the school's ethos, school's staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of School Devices and Systems

4. I will only use the equipment and internet services provided to me by the school, for example school provided laptops, tablets, mobile phones and internet access, when working directly with learners. Personal devices should not be used when working with learners.
5. I understand that any equipment and internet services provided by my workplace are intended for use in carrying out my professional duties and should only be accessed by members of staff. Reasonable personal use of James Dixon Primary School's IT systems and/or devices by staff is allowed.

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. I will not allow a third party to use a school device provided to me and will ensure I do not leave school devices unsupervised in public places.
 - I will not allow any student to use a school device provided to me or any other staff member.
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 team.
 9. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT team.
 10. I will ensure that any personal data is kept in accordance with the Data Protection legislation, in line with the Trust Data Protection Policy.
 - 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.
 11. I will use email communication professionally and understand that anything written in email can be shared with other professionals and/or parents/carers at any time. I will not use email to conduct private conversations with a third party.
 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. I will only use the school's learning environment to upload any work documents and files in a password protected environment.
 13. I will not store any personal information on the school IT system, including school laptops or similar devices 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 IT team as soon as possible.
 17. If I have lost any school related documents or files, I will report this to the IT team and school Data Protection Officer as soon as possible.
 18. Any images or videos of learners will only be used for school purposes.

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

Classroom Practice

19. I am aware of safe technology use in the classroom and other working spaces, including appropriate supervision of learners, as outlined in the school online safety policy.
20. I have read and understood the school's online safety policy which covers expectations for learners regarding mobile technology and social media.
21. I will promote online safety with the learners in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
 - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used on site.
 - creating a safe environment where learners feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
 - involving the Designated Safeguarding Lead (DSL) or a deputy DSL as part of planning online safety lessons or activities to ensure support is in place for any learners who may be impacted by the content.
 - make informed decisions to ensure any online safety resources used with learners are appropriate.
22. I will report any filtering breaches (such as access to illegal, inappropriate or harmful material) to the DSL in line with the school's online safety/child protection and safeguarding policy.
23. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text or music are protected, I will not copy, share or distribute or use them.

Use of Social Media and Mobile Technology

24. I have read and understood the school's online safety policy which covers expectations regarding staff use of mobile technology and social media.
25. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role and in line with the staff code of conduct, when using school and personal systems. This includes my use of email, text, social media and any other personal devices or mobile technology.
 - I will take appropriate steps to protect myself online when using social media as outlined in the online safety policy.
 - I am aware of the school expectations with regards to use of personal devices and mobile technology, including mobile phones as outlined in the online safety policy.
 - I will not discuss or share data or information relating to learners, staff, school business or parents/carers on social media.
 - I will ensure that my use of technology and the internet does not undermine my professional role or interfere with my work duties and is in accordance with the school code of conduct and the law.

26. My electronic communications with current and past learners and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
- I will ensure that all electronic communications take place in a professional manner via school approved and/or provided communication channels, such as a school email address or telephone number.
 - I will not share any personal contact information or details with learners, such as my personal email address or phone number.
 - I will not add or accept friend requests or communications on personal social media with current or past learners and/or parents/carers.
 - If I am approached online by a learner or parents/carer, I will not respond and will report the communication to my line manager and Designated Safeguarding Lead (DSL).
 - Any pre-existing relationships or situations that compromise my ability to comply with the AUA will be discussed with the DSL and/or headteacher.
27. 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 headteacher.
28. 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.
29. 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.
30. 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.

Agreement Compliance

31. I understand that the school may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor agreement compliance and to ensure the safety of learners and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

Policy Breaches or Concerns

32. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the DSL in line with the school's online safeguarding and child protection policy.
33. I will report concerns about the welfare, safety or behaviour of staff to the headteacher, in line with the whistleblowing policy.
34. I understand that if the school believes that unauthorised and/or inappropriate use of school systems or devices is taking place, the school may invoke its disciplinary procedures as outlined in the Staff Discipline and Conduct policy.

35. I understand that if the school believes 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 Discipline and Conduct policy.

36. 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 the James Dixon Primary School Staff Acceptable Use of Technology Agreement when using the internet and other associated technologies, both on and off site.

Name of staff member:

Signed:

Date (DDMMYY).....