

# Acceptable Use of Technology for Staff, Visitors and Volunteers Statements

## Staff Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Ditton Junior 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 learners, 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 Ditton Junior School expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that Ditton Junior 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 AUP applies to my use of technology systems and services provided to me or accessed as part of my role within Ditton Junior 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, remote learning and online and offline communication technologies.
2. I understand that Ditton Junior School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the Ditton Junior School staff code of conduct.
3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the Ditton Junior School ethos, Ditton Junior School staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

### Use of Ditton Junior School Devices and Systems

4. I will only use the equipment and internet services provided to me by Ditton Junior School for example provided laptops, tablets, mobile phones, and internet access, when working with learners.

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 devices by staff is allowed. Occasional personal use of the settings devices is considered as beneficial to the development of staff IT skills and enables staff to maintain a positive work-life balance. However, this is at the setting's discretion and can be revoked at any time. This use must remain within reasonable boundaries.
6. Where I deliver or support remote learning, I will comply with the Ditton Junior School remote learning AUP.

## **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 Ditton Junior 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.
8. I will respect Ditton Junior 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 Headteacher/Deputy Headteacher.
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 and Headteacher.
11. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the Ditton Junior 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 Ditton Junior School site, such as via email or on memory sticks or CDs, will be suitably protected. This may include

data being encrypted on a password protected memory stick, approved by Ditton Junior School.

12. Where possible, I will use the Ditton Junior School learning platform to upload any work documents and files in a password protected environment or Ditton Junior School approved/provided VPN.
13. I will not store any personal information on the Ditton Junior School IT system, including Ditton Junior School laptops or similar device issued to members of staff, that is unrelated to Ditton Junior School activities, such as personal photographs, files or financial information.
14. I will ensure that Ditton Junior 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 Ditton Junior 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 Ditton Junior School related documents or files, I will report this to the Headteacher and Ditton Junior School Data Protection Officer (Cantium Business Solutions) as soon as possible.
18. I understand images of learners must always be appropriate and should only be taken with Ditton Junior School provided equipment and only be taken/published where learners and/or parent/carers have given explicit written consent.

## **Classroom Practice**

19. 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 child protection policy, online safety policy and remote learning AUP
20. I have read and understood the Ditton Junior School mobile technology and social media policies.
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.
- creating a safe environment where learners 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) Ruth Campbell, or a deputy, Kelli Moon or Kirstie Semark, 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 is appropriate.

22. I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL in line with the Ditton Junior School child protection policies.

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.

### **Mobile Devices and Smart Technology**

24. 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.

### **Online Communication, including Use of Social Media**

25. 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 code of conduct and the law:

- I will take appropriate steps to protect myself and my reputation online when using communication technology, including the use of social media as outlined in the social media policy.
- I will not discuss or share data or information relating to learners, staff, Ditton Junior School business or parents/carers on social media.

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 Ditton Junior School approved and/or provided communication

channels and systems, such as a Ditton Junior School email address, user account, telephone number, or Class Dojo

- 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 their parents/carers.
- If I am approached online by a current or past learner or parents/carer, I will not respond and will report the communication to my line manager and Designated Safeguarding Lead (DSL). (Ruth Campbell)
- Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the DSL and Headteacher.

## **Policy Concerns**

27. 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.

28. 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.

29. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the Ditton Junior School into disrepute.

30. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the DSL in line with the Ditton Junior School child protection policy.

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

## **Policy Compliance and Breaches**

32. If I have any queries or questions regarding safe and professional practise online either in Ditton Junior School or off site, I will raise them with the DSL and the Headteacher

33. I understand that Ditton Junior School may exercise its right to monitor the use of its information systems, including internet access and the interception of emails, to monitor policy 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.

34. I understand that if Ditton Junior School believe that unauthorised and/or inappropriate use of Ditton Junior School systems or devices is taking place, Ditton Junior School may invoke its disciplinary procedures as outlined in the staff code of conduct.

35. I understand that if Ditton Junior School believe that unprofessional or inappropriate online activity, including behaviour which could bring Ditton Junior School into disrepute, is taking place online, Ditton Junior School may invoke its disciplinary procedures as outlined in the staff code of conduct.

36. I understand that if Ditton Junior School suspects criminal offences have occurred, the police will be informed.

**I have read, understood and agreed to comply with Ditton Junior 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).....