Dry Drayton C.E (C) Primary School

Staff Acceptable Use Policy

Dry Drayton C.E (C) Primary School	
Title	Staff Acceptable Use Policy
Date	23rd January 2023
Approved by Head teacher	23rd January 2023
Approved by governing body	23rd January 2023
Next review date	23rd January 2026

Contents

Staff Acceptable Use Policy

This policy covers the following aspects of ICT and e-safety in relation to all school staff:

- Use of school-based equipment
- Social Networking
- Managing digital content
- Email
- Personal Mobile phones and devices
- Learning and teaching

All staff should read and sign this document to demonstrate that they agree with the statements.

1. Use of school-based equipment

When using the school's ICT equipment and other information systems, I have understood and will comply with the following statements

1. I will access the internet and other ICT systems using an individual username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any suspicion, or evidence that there has been a breach of my personal security in relation to access to the internet or ICT systems, to the Head Teacher.
2. All passwords I create will be in accordance with the school e-safety Policy. I will ensure that I use a suitably complex password for access to the internet and ICT systems.
3. I will not share my passwords.
4. I will seek consent from the Headteacher prior to the use of any new technologies (hardware, software, cloud-based services) within school.
5. I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material, I will report it immediately to the Headteacher.
6. I will take a professional and proactive approach to assessing the effectiveness of the internet content-filtering platform in relation to the educational content that can be viewed by the pupils in my care.
7. 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 office manager.
8. I understand my personal responsibilities in relation to the Data Protection Act & GDPR 2018 and the privacy and disclosure of personal and sensitive confidential information.
9. I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car overnight or left in sight when not in use, e.g. by an open window or on the back seat of a car.
10. I will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption/ password protection deployed.

11. Any information asset, which I create from other information systems, which could be deemed as personal or sensitive will be stored on the school network and access controlled in a suitable manner in accordance with the school data protection2018 controls. (For example spreadsheets /other documents created from information located within the school information management system).
12. I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it without prior authorisation from the Head Teacher.
13. I understand that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities. Remote systems will only be accessed by authorised members of staff using secure logons and secondary authentication methods e.g. key fobs.
14. I understand that my files, communications and internet activity may be monitored and checked at all times to protect my own and others' safety, and action may be taken if deemed necessary to safeguard me or others.

2. Social Networking

1. I must not talk about my professional role in any capacity when using personal social media such as Facebook, Twitter and YouTube or any other online publishing websites.
2. I must not use social media tools to communicate with current or former pupils under the age of 18.
3. I will not use any social media tools to communicate with parents in a professional capacity and I will take all reasonable steps to ensure any online communication will not damage the school's reputation.
4. I will set and maintain my profile on social networking sites to appropriate privacy levels and allow access to known friends only.
5. Staff must not access social networking sites for personal use during school hours.

3. Managing digital content

1. I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school.
2. I will only use school equipment to create digital images, video and sound. Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress. No resources will be published online without the permission/consent of the staff and parents/carers of pupils involved as detailed in the e-safety Policy and Home School Agreement.
3. Under no circumstances will I use any personally owned equipment for video, sound or images without prior consent from a member of the Senior Leadership Team.
4. When searching for images, video or sound clips, I will ensure that I or any pupils in my care are not in breach of any copyright licencing.
5. I will ensure that any images, videos or sound clips of pupils are stored on the school network and never transferred to personally owned equipment.
6. I will ensure that any images taken on school-owned devices will be transferred to the school network (storage area/server) and deleted as soon as possible from the memory card.
7. I will model safe and responsible behaviour in the creation and publishing of online content within the school learning platform and any other websites. In addition to this I will encourage colleagues and pupils to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

4. Email

1. Communication to parents/carers should be through the schools secure 'communication system' i.e. parent mail, Class Dojo; if MS Outlook email is used for multiple parents, email addresses or distributions lists should be via the blind copy (bcc) field.
2. I will use my school email address for all correspondence with staff and other agencies. I understand that any use of the school email system will be monitored and checked. I will under no circumstances use my private email account for any school-related business.
3. Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
4. I will seek permission if I need to synchronise any school email account with a personally owned handheld device and ensure that the device has a pin code to access.
5. I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.
6. Emails sent to external organisations will be written carefully and if necessary authorised before sending to protect myself. As and when I feel it necessary, I will carbon copy (cc) the head teacher, line manager or another suitable member of staff into the email.
7. I will ensure that I manage my email account, delete unwanted emails and file those I need to keep in subject folders.
8. I will access my school email account on a regular basis to ensure that I respond in a timely manner to communications that require my attention.

5. Personal mobile phones and devices

1. I will ensure that my mobile phone and any other personally owned device is switched off or switched to 'silent' mode and out of sight during the school day.
2. Bluetooth, AirDrop and other wireless communication channels should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances.
3. I will only contact any parents or pupils on my personally owned device through the accepted platforms of Seesaw and ClassDojo
4. I will not use any personally owned mobile device to take images, video or sound recordings of children or their work.
5. I will use my mobile/device in line with the school mobile phone, cameras and technological device policy.

6. Learning and teaching

1. In line with every child's legal entitlement I will ensure I teach an age appropriate e-safety curriculum.
2. I will support and promote the school e-safety policy at all times. I will model safe and responsible behaviour in pupils when using technology to support learning and teaching.
3. I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
4. I understand the importance of respecting and acknowledging copyright of materials found on the internet and will strive to model best practice in the creation of my own resources at all times.

7. Agreement

I have read and understood the implications and my personal responsibilities in relation to the use of ICT equipment which is detailed within this policy.

I understand that if I fail to comply with this Acceptable Use Policy agreement, I could be subject to disciplinary action.
Name :
Role in School:
Signed
Date:
Accepted by:
Date: