

**Acceptable Use Agreement – Staff**

 [Insert School Name]

[Version 2.0]

|  |  |
| --- | --- |
| **Last Reviewed** |  |
| **Reviewed By (Name)** |  |
| **Job Role** |  |
| **Next Review Date** |  |
| **Version released Spring 2024** | Reviewed and updated in light of DfE Digital Standards |

This document will be reviewed annually and sooner when significant changes are made to the law.

Guidance from the Department for Education about school policies can be found here: <https://www.gov.uk/government/publications/statutory-policies-for-schools-and-academy-trusts/statutory-policies-for-schools-and-academy-trusts>

# 1.1 Introduction

Everyone who works for [Insert school name] school has a responsibility to ensure that data is collected, accessed, stored and handled appropriately and lawfully. Every user must ensure that they adhere to the following statements in order to meet the legal obligations of the school and their individual obligations.

All members of staff are expected to abide by relevant school policies. Special consideration should be given to the following:

· Data Protection Policy

· IT Security Policy

· Acceptable Use Policy

· Bring Your Own Device (BYOD) Policy

· Online Safety Policy.

# 1.2 IT Acceptable Use Standards

All Users must:

1. Protect school IT resources by careful and considerate use of equipment and networks, reporting faults and minimising the risk of introducing computer viruses or similar to the system.
2. Protect individuals from harmful or inappropriate material accessible via the Internet or electronic media.
3. Protect the confidentiality of individuals and of school matters and safeguard Users by complying with relevant legislation, including, but not limited to:
* Data Protection Act 2018 and UK General Data Protection Regulation
* Privacy and Electronic Communications Regulations
* Copyright, Designs and Patent Act 1988
* Computer Misuse Act 1990
* Counter-Terrorism and Security Act 2015 (encompassing the “Prevent Duty”)
* The Regulation of Investigatory Powers Act (RIPA) 2000
* Waste Electrical and Electronic Equipment Regulations 2006, the Environmental Protection Act 1990, the Waste Management Regulations 2006.
* The Department for Education [Digital and Technology Standards for Schools and Colleges](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges)
* Keeping Children Safe in Education (KCSIE)

Users should understand and adhere to their signed Acceptable Use Agreement.

# 1.3 Agreement Statements

[Advise staff where copies of relevant policies may be attained or insert link to the school website here.]

1. I have read, understand and agree to abide by [ insert school name ]’s

* Acceptable Use Policy
* Online Safety Policy
* Social Media Policy
* Data Protection Policy
* Bring Your Own Device (BYOD) Policy

2. I will follow Keeping Children Safe in Education (KCSIE) guidance and I have read the sections on handling incidents and concerns about a child in general, sexting, upskirting, bullying, sexual violence and harassment, misuse of technology, and social media.

3. I will conduct myself in a professional manner and be professionally dressed at all times, including when conducting virtual / remote lessons and/or meetings. I will log any issues or concerns if anything inappropriate happens during live / online lessons to safeguard myself and pupils.

4. I understand that it is my responsibility to support the safeguarding of pupils and other staff and I will report any actions or behaviour which I believe is inappropriate, or could lead to individuals being placed at risk, to [insert relevant staff member / role], without delay.

5. I will not contact or attempt to contact any pupil in any way other than school-approved and school-monitored ways. Please advise the headteacher if you are socially connected to pupils as a relative/family friend.

6. I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I will respect others who may have differing opinions.

7. I will never use school devices and networks / internet / platforms / other technologies to browse, access, download or send material that is offensive, extremist, illegal, or in any way inappropriate for an educational setting.

8. I understand the importance of upholding my online reputation, my professional reputation, and that of the school, and I will do nothing to impair them.

9. I will not arrange or attempt to create any remote / virtual meetings, lessons, or similar online communications without the prior knowledge and approval of the school. I will not record or take screenshots of myself or pupils during lessons / meetings, unless the purpose is made clear to all parties and the need has been established and approved by senior staff.

10. I will not store school-related data on personal devices, storage, or cloud platforms.

11. I will not access, attempt to access, store, or share any data which I do not have express permission for. I will check all permissions prior to any uploading or sharing images of others.

12. I will ensure that data I am responsible for is regularly backed up, in accordance with relevant school / academy policies. This includes backing up data on portable storage devices, if appropriate.

13. I will only use complex passwords and not use the same password across different platforms / systems. I will protect and never share my credentials. If I suspect a breach I will immediately change passwords and notify [insert relevant staff member / role].

14. I understand that school systems and users are protected by security, monitoring, and filtering services, and that my use of school devices, systems, and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored / captured / viewed by the relevant authorised staff members.

15. I will not attempt to bypass security or monitoring and will report any damage, loss or malfunction of any devices loaned to me.

16. [Schools to delete if your BYOD policy does not allow personal devices] When using my own devices on school premises or accessing school systems / platforms, I will ensure I take appropriate steps to safeguard and secure my device.

17. USB sticks / pen drives will be encrypted and virus checked prior to use. [Remove this if school prohibits these]

18. I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others. I will report any suspected damage, regardless of the cause, to [insert relevant staff member / role].

19. In order to protect personal data and sensitive information, I will use ‘Extend’ screen and not ‘Duplicate’, when projecting / connecting from devices to whiteboards / additional screens.

20. I will report any suspected security incidents, notifications, or security alerts from antivirus systems, firewalls, or malware protection, promptly, to [insert relevant staff member / role].

21. I will only use safe and appropriately licensed software. I will respect licensing and intellectual property rights / copyright. Where work is protected by copyright, I will not download or distribute copies, including music and videos.

22. I understand that breach of this agreement may lead to appropriate staff disciplinary action or termination of my contract. Where appropriate, there may be a referral to other relevant authorities.

I understand these restrictions apply when accessing a platform or the school network from any device or location (in and out of school) and to the transfer of personal data (digital or paper based).

Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Role:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

I approve this user to be allocated credentials for school systems as relevant to their role.

Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Role:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Amend a complete list of systems the user has been given access to, and the level of access provided.

Users should also be advised how to report and respond to suspected incidents.