



Aintree Davenhill Primary

Visitor & Contractor Acceptable Use Agreement (AUA)

ICT (including data) and the related technologies such as e-mail, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that visitors & contractors working in school are aware of their professional responsibilities when using any form of ICT. Visitors & Contractors are expected to adhere to this policy. Any concerns or clarification should be discussed with a member of the SLT.

Introduction

As a visitor / contractor to Aintree Davenhill you may be given access to school devices or networks to aid the provision of your services or your support to pupils and staff of the school. You are required to agree to the conditions of this document prior to accessing the school systems.

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

- Data Protection Policy
- Cyber Security Policy
- Staff and Pupil Acceptable Agreement Policies
- Online Safety Policy.

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 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](#)

- Keeping Children Safe in Education (KCSIE)

Users should understand and adhere to this Acceptable Use Agreement.

Agreement Statements

1. Any observations, incidents, or conversations taking place during my time in school will be kept confidential.
2. I understand that it is my responsibility to support the safeguarding of pupils and other staff. If I have any Child Protection or Safeguarding concerns, or if I am asked to do something, or see something I consider not best practice, I will report this to the Head teacher.
3. I understand the importance of upholding my online reputation, my professional reputation, and that of the school, and I will do nothing to impair these. I will conduct myself in a professional manner, including professional dress and always using appropriate language.
4. I will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school. I will not contact or attempt to contact any pupil in any way other than school-approved and school-monitored ways.
5. I will not store school-related data on personal devices, storage, or cloud platforms.
6. I will not access, attempt to access, store, or share any data which I do not have express permission for.
7. I will not share any information about the school or members of its community gained during my visit, verbally, electronically, or via social media in any way, or on any platform, except where relevant to the purpose of my visit and agreed in advance with the school.
8. I will not take photographs or videos whilst on site unless the purpose has been communicated to senior leaders and prior permission has been granted. (e.g., to take photos of equipment or buildings)
9. I understand that school systems and users are protected by security, monitoring, and filtering services, and that my use of school devices and systems can be monitored/captured/viewed by the relevant authorised staff members.
10. School-owned devices, networks, cloud platforms or other technology, will be used exclusively for the purposes to which they have been assigned to me, and not for any personal use. I will not attempt to bypass security or monitoring, and will look after devices I have been given authorised use of.
11. 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.
12. USB sticks / pen drives are not authorised unless permission has been sought from the DPO or the SLT Digital Lead (Remember these are a considerable security risk from outside your network.)
13. I will report any suspected security incidents, notifications, or security alerts from antivirus systems, firewalls, or malware protection, promptly, to the Head teacher.

I understand that breach of this agreement may lead to appropriate immediate termination of any contracts and, when necessary, referral to other relevant authorities.

I have read, understood, and agree to the conditions of the acceptable use agreement for IT and the Internet of Aintree Davenhill.

Key contacts in school:

Role	Name	Email
Head teacher	Emma Clay	Head.aintreedavenhill@schools.sefton.gov.uk
Safeguarding Lead	Emma Clay	Safeguarding.aintreedavenhill@schools.sefton.gov.uk
Deputy Safeguarding Lead	Emma Taylor Kate Siveyer	eyfs.aintreedavenhill@schools.sefton.gov.uk senco.aintreedavenhill@schools.sefton.gov.uk
Administration Link	Jennifer Molloy	Admin.aintreedavenhill@schools.sefton.gov.uk

Visitor / Contractor Concern Form

Part 1 - to be completed by the person raising concern	
Name of Visitor / Contractor:	
Date and time:	
Summary of concern and any known details:	
Does it involve any individuals?	
If so, can you provide names?	
Any action taken so far: <i>Please include other staff members aware of the issue and any witnesses.</i>	
What type of concern is this?	Safeguarding Concern Security Incident Unauthorised Use Illegal Activity Breach of policy

Please pass this concern form to the Headteacher

Part 2 – to be completed by Headteacher	
Date and time received:	
Outcomes and Actions <i>Record any contact with Action Fraud / Police Cyber Protection Officers / IT Provider etc.</i> <i>If this information is transferred to CPOMS, state this and add any reference.</i>	
<u>In the case of safeguarding concerns this record should be retained by the DSL.</u>	
Part 3 – to be completed by DSL	
Date and time received:	
DSL initial:	
CP concern: YES / NO	
Starting Point referral: YES /NO	
Is this a concern under Prevent: YES / NO	
If YES: Complete Prevent Risk Indicator Checklist	
Further actions taken: <i>Record all strategies agreed including school based ones, and record an outcome including evidence of referrals/agreement with agencies.</i>	
Have parents/carers been contacted? YES / NO	
If NO, provide justification here: <i>In all cases except where there is clear evidence of putting a child at immediate risk, parents/carers should be contacted.</i>	
Feedback to Referrer YES/NO	
Date closed:	