

ACKLAM GRANGE SCHOOL



IT Acceptable Use Policy

Status & Review Cycle	Term	Year
Last Review Date/Policy Adopted	Summer Term	2025-26
Next Review Date	Summer Term	2026-27
Lead	Mr A Fletcher	

This school is an academy within The Legacy Learning Trust.



I.T. Acceptable Use Policy (AUP) 2026-2027 - Staff

The school has the responsibility for providing all staff with safe, reliable and useful I.T. resources (network access, internet access, virtual learning environment etc.). Staff have a right to these resources. With this right however, come the following responsibilities:

1. Internet Access

Staff must not access, or attempt to access, websites that contain or promote any of the following: extremism and radicalisation, child abuse, pornography, discrimination of any kind, racial or religious hatred, illegal acts and any other information which may be illegal or offensive to colleagues, unless it is a recognised part of the taught curriculum and permission has been granted by a member of the Senior Leadership Team. It is recognised that under certain circumstances inadvertent access may happen. Should a member of staff access any of these sites unintentionally they should report the matter to the IT Services team so that it can be logged, and appropriate action taken if required.

2. Wireless Access

Staff can gain access to the school's wireless provision on their personal devices by contacting the IT Services team. Staff must ensure that they use the school wireless access appropriately at all times.

3. Inappropriate/Illegal Content

Access to any of the following should be reported to the police:

- Images/videos of child sexual abuse (sometimes incorrectly referred to as child pornography). These are images/videos of children apparently under 18 years old involved in sexual activity or posed to be sexually provocative.
- Adult material that potentially breaches the Obscene Publications Act
- Criminally racist material in the UK.

4. Social Networks

The school's expectation of employees is that they do not connect socially with students via social media or other communication channels. The school will make exceptions to this in the case of immediate family members only.

Staff are strongly encouraged to set their personal social media accounts to private. Where accounts are publicly accessible, staff must ensure that any content posted is consistent with the professional standards expected of school employees and does not bring the school into disrepute. Staff should be aware that, as employees of the school, their online presence may reflect on the school and they are expected to uphold the school's values and standards when using public social media platforms.

Our school is part of our community and we recognize that, as members of the community, staff will come into contact with students outside of the school. We expect staff to use their professional judgement in such situations and to report to their line manager any contact that they have had with a student, outside of school, that they are concerned about or that could be misinterpreted by others.

5. Communication

Staff should only communicate directly with students electronically for legitimate school-related purposes using school-approved systems such as Class Charts Messages, School Email and the Office 365 Teams platform. All communication conducted through these systems must be professional, appropriate, and consistent with the school's standards of conduct and expectations for staff-student interactions.

If there are any circumstances in which an employee has to provide their personal contact details,

including phone numbers, email addresses or other personal communication details, to any student, they must report this to the Headteacher.

When communicating with other staff, parents or carers, employees should use systems provided and managed by the school wherever practicable. All communications must be professional in tone and content and consistent with the school's expectations for professional conduct.

- The AGS school email system is to be used as the 'priority system' for communication between staff on professional matters.
- AGS school email may be used for communication between staff and parents for educational matters of a high priority however telephoning home will continue to be the primary method for staff to communicate with parents.
- School email accounts must not be used for personal purposes.

6. Remote Working

Staff should utilize Microsoft OneDrive and Teams where possible to store their documents and to access them remotely. Staff are permitted access to their OneDrive accounts, Teams and other shared areas using Microsoft office 365. Staff are also able to access the Management Information System, Arbor, remotely.

It is essential that staff ensure full compliance with data protection and do not leave home computers or other computer devices unattended when logged in. Sensitive data should not be saved to personal computer devices under any circumstances.

7. Passwords

It is important that staff passwords are kept private. Passwords are confidential and individualised to each person. On no account should a member of staff allow anybody else to use their login (particularly students).

A strong password should be used – a password should be a minimum of 8 characters in length (we would encourage this to be longer), contain upper and lower case alphabetical characters and numbers or punctuation characters. If a member of staff knows or suspects that another person has obtained or is aware of their password, they must contact the IT team immediately so that appropriate action can be taken to secure their account.

Multi-Factor Authentication (MFA) will be enabled for all staff on supported school systems, including Office 365, CPOMS and Arbor.

8. Data Protection

Staff should adhere to the Data Protection Policy at all times. Where a member of staff has to take home sensitive or confidential information, sufficient safeguards should be in place to prevent loss or misuse. If flash drives (USB pens) or external hard drives are used these should be encrypted. All data relating to staff, students and parents must be kept private and confidential. No school related data, documents or images should be stored on personal computer devices under any circumstances.

9. Copyright

Staff must ensure that their work does not break the Copyright, Design and Patents law.

10. Personal Use

Staff are not permitted to use school I.T. equipment for personal use without Senior Leadership Team approval. If personal use is permitted the boundaries of use should be written down and adhered to.

11. File Storage

Staff must only store school-related files and images in the network areas and OneDrive/Teams storage areas they have access to.

12. Images and Videos

- No images or videos should ever be uploaded to a website or social network, without photo consent being given. This can be checked in Arbor. Similarly, no personal information other than the students first name should ever be shared.

13. Use of Personal I.T. devices / Bring Your Own Devices (BYOD)

- Use of personal I.T. equipment (mobile phones, tablets, cameras, personal laptop etc.) is at the discretion of the Senior Leadership Team. Any such use should be stringently checked for up to date anti-virus and malware checkers. Use of personal I.T. devices is subject to the same Acceptable Use Policy.
- Pictures or videos of AGS students should be taken with a school camera if at all possible. On occasion, staff will need to take photographs and videos of school related events using personal devices. In this situation the images or videos should be transferred from the device onto the school network within 72 hours and completely removed from the personal device.

14. Reporting Concerns

It is the duty of staff to support the school's safeguarding policy and report any behaviour (staff or students), which is inappropriate or a cause for concern, to a member of the Safeguarding Team.

15. Monitoring

All staff should be aware that monitoring systems are in place on all school devices. These systems monitor the use of school networks and services, including email communications, internet activity, and the creation, modification, and storage of documents and files.

School devices remain subject to monitoring when used off-site, including when connected to a home Wi-Fi network.

As part of the staff induction process new staff are made aware of the systems, how they work and the implications on their use of the school's IT facilities.

16. Printing and Copying

Staff should always '**Think before they Print**' and where possible use alternative methods to printing. When printing, staff should only print in colour where absolutely necessary.

17. Data Protection

I will adhere to the Data Protection Act (2018), the schools Data Protection Policy, and the Computer Misuse Act (1990) at all times. Links to view these documents can be found on the school website.