Staff Acceptable Use Policy

Revision 1.4

Date of last review: August 2024

Guidelines for Staff

The Academy has provided computers for use by staff as an important tool for teaching, learning, and administration of the Academy. Use of Academy computers by staff is governed at all times by the following policy. Please ensure you understand your responsibilities under this policy, and direct any questions or concerns to the IT Support Team in the first instance.

All members of staff have a responsibility to use the Academy's computer system in a professional, lawful, and ethical manner. Deliberate abuse of the Academy's computer system may result in disciplinary action (including possible termination), and civil and/or criminal liability.

Please note that use of the Academy network is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the Academy and staff, to safeguard the reputation of the Academy, and to ensure the safety of all users. Please respect these guidelines, many of which are in place for your protection.

Lastly, the Academy recognises that the distinction between computer use at work and at home is increasingly blurred, with many of us now using our own computers for work. While the Academy neither wishes nor intends to dictate how you use your own computer, staff should consider that the spirit of this policy applies whenever you are undertaking an activity that stems from your employment with the Academy.

Computer Security and Data Protection

- You will be provided with a personal account for accessing the computer system, with your own username and password. This account will be tailored to the level of access you require, and is for your use only. As such, you must not disclose your password to anyone, including IT Support staff. If you do so, you will be required to change your password immediately.
- You must not allow a pupil to have individual use of a staff account under any circumstances, for any length of time, even if supervised.
- When leaving a computer unattended, you must ensure you have either logged off your account, or locked the computer to prevent anyone using your account in your absence.
- You must not store any sensitive or personal information about staff or students on any portable storage system (such as a USB memory stick, portable hard disk, or personal computer) unless that storage system is encrypted and approved for such use by the Academy IT Support Team.
- You must not transmit any sensitive or personal information about staff or students via email without the data being encrypted by a method approved by the Academy IT Support Team.
- When publishing or transmitting non-sensitive material outside of the Academy, you must take steps to protect the identity of any pupil whose parents have requested this.

- If you use a personal computer at home for work purposes, you must ensure that any Academy related sensitive or personal information is secured to prohibit access by any non-member of staff, and encrypted to protect against theft.
- You must make your own backup of data kept on any storage system other than the network storage drives or your 'My Documents' folder. This includes USB memory sticks (even those owned or issued by the Academy) or a personal computer.
- You must ensure that items of portable computer equipment (such as laptops, digital cameras, or portable projectors) are securely stored in a locked room or cupboard when left unattended.
- Equipment taken offsite is not routinely insured by the Academy. If you take any Academy computer equipment offsite, you should ensure that adequate insurance cover has been arranged to cover against loss, damage, or theft including any laptops issued for staff use.

Personal Use

The Academy recognises that occasional personal use of the Academy's computers is beneficial both to the development of your IT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use:

- must comply with all other conditions of this AUP as they apply to non-personal use, and all other Academy policies regarding staff conduct;
- must not interfere in any way with your other duties or those of any other member of staff;
- must not have any undue effect on the performance of the computer system; and
- must not be for any commercial or political purpose or gain unless explicitly authorised by the Academy.
- Personal use is permitted at the discretion of the Academy and can be limited or revoked at any time.

Use of your own Equipment

- Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff, and must not be used until approved. This test must be performed at regular intervals as required by Academy's normal rules on electrical safety testing.
- You must not connect personal computer equipment to Academy computer equipment without prior approval from IT Support staff in writing, with the exception of storage devices such as USB memory sticks.
- If you keep files on a personal storage device (such as a USB memory stick), you must ensure that other computers you connect this storage device to (such as your own computers at home) have an up-to-date anti-virus system running to protect against the proliferation of harmful software onto the Academy computer system.

Conduct

- You must at all times conduct your computer usage professionally, which includes being polite and using the system in a safe, legal and business appropriate manner. Among uses that are considered unacceptable are the following:
    - Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;
    - Making ethnic, sexual-preference, or gender-related slurs or jokes.

- You must respect, and not attempt to bypass, security or access restrictions in place on the computer system.
- You must not intentionally damage, disable, or otherwise harm the operation of computers.
- You must make efforts not to intentionally waste resources. Examples of resource wastage include:
    - Excessive storage of unnecessary files on the network storage areas;
    - Use of computer printers to produce class sets of materials, instead of using photocopiers.
- You should avoid eating or drinking around computer equipment.

Use of Social Networking websites and online forums

If permitted by the Academy, staff must take care when using social networking websites such as Facebook, Twitter, LinkedIn or Instagram, even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.

You must not allow any pupil to access personal information you post on a social networking site. In particular:

- You must not add a pupil to your 'friends list' (or similar).
- You must ensure that personal information is not accessible via a 'Public' setting, but ensure it is set to a 'Friends only' level of visibility.
- You should avoid contacting any pupil privately via a social networking website, even for Academy-related purposes.
- You should take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them access to your personal information.
- Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the Academy – even if their online activities are entirely unrelated to the Academy.

- Unless authorised to do so, you must not post content on websites that may appear as if you are speaking for the Academy.
- You should not post any material online that can be clearly linked to the Academy that may damage the Academy's reputation.
- You should avoid posting any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass, or defame the subject.

Use of Email

All members of staff with a computer account are provided with an email address for communication both internally and with other email users outside the Academy. The following considerations must be made when communicating by email:

- E-mail has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of e-mails may therefore have to be made available to third parties. You must be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for e-mail.
- E-mail to outside organisations has the same power to create a binding contract as hardcopy documents. Check e-mail as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal advice before sending. You must not purchase goods or services on behalf of the Academy via e-mail without proper authorisation.
- All Academy e-mail you send should have a signature containing your name, job title and the name of the Academy.
- E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, you must not send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential information belonging to the Academy.
- Having an external e-mail address may lead to receipt of unsolicited e-mail containing offensive and/or sexually explicit content. The Academy will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users from the Internet.
- You must not send chain letters or unsolicited commercial e-mail (also known as SPAM).

Use of E-Learning Platforms

Google Classroom and/or Microsoft Classroom (Teams) are the E-Learning Platforms provided by the academy, accessible to staff and students. These platforms must only be used to aid teaching and learning and for no other function. The following considerations must be made when using the E-Learning Platforms:

- The platforms have elements of social networking and therefore the guidelines mentioned in 'Use of Social Networking websites and online forums' apply.
- You must not post or store personal information or pupil information on the platform.
- You are responsible for the management of your data including retrieval of deleted posts and data. Data on the platforms is not backup by the academy.
- It is the sole responsibility of staff to make sure student work is backed up and transferred onto the academy's file server.

Supervision of Pupil Use

- Pupils must be supervised at all times when using Academy computer equipment. When arranging use of computer facilities for pupils, you must ensure supervision is available.
- Supervising staff are responsible for ensuring that the separate Acceptable Use Policy for pupils is enforced.
- Supervising staff must ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of computer use by pupils.

Privacy

- Use of the Academy computer system, including your email account and storage areas provided for your use, may be subject to monitoring by the Academy to ensure compliance with this Acceptable Use Policy and applicable laws. This may include remote monitoring of an interactive logon session. In particular, the Academy does keep a complete record of sites visited on the Internet by both pupils and staff and logs of all email messages. Usernames and passwords used on those sites are NOT monitored or recorded.
- You should avoid storing sensitive personal information on the Academy computer system that is unrelated to Academy activities (such as personal passwords, photographs, or financial information).
- The Academy may also use measures to audit use of computer systems for performance and diagnostic purposes.
- Use of the Academy computer system indicates your consent to the above described monitoring taking place.

Confidentiality and Copyright

- Respect the work and ownership rights of people outside the Academy, as well as other staff or pupils.
- You are responsible for complying with copyright law and licenses that may apply to software, files, graphics, documents, messages, and other material you wish to use, download or copy. Even if materials on the Academy computer system or the Internet are not marked with the copyright symbol (©), you should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.
- You must consult a member of IT Support staff before placing any order of computer hardware or software, any computer peripheral or obtaining and using any software you believe to be free. This is to check that the intended use by the Academy is permitted under copyright law (as well as to check compatibility and discuss any other implications that the purchase may have). Do not rely on the claims of suppliers, who do not have specific knowledge of the Academy's systems.
- As per the standard staff contract, any invention, improvement, design, process, information, copyright work, trade mark or trade name made, created or discovered by you during the course of your employment in any way affecting or relating to the business of the Academy or capable of being used or adapted for use within the Academy shall be immediately disclosed to the Academy and shall to the extent permitted by law belong to and be the absolute property of the Academy.
- By storing or creating any personal documents or files on the Academy computer system, you grant the Academy a non-exclusive, universal, perpetual, irrevocable, and royalty-free license to

use, copy, and distribute those documents or files in any way the Academy sees fit.

Reporting Problems with the Computer System

It is the job of the IT Support Team to ensure that the Academy computer system is working optimally at all times and that any faults are rectified as soon as possible. To this end:

- You should report any problems that need attention to a member of IT Support staff via the Parago Helpdesk System as soon as is feasible. Problems that seriously hinder your job or teaching and require immediate attention should be reported by telephone or email; any other problem must be reported via the Parago Helpdesk System.
- If you suspect your computer has been affected by a virus or other malware, you must report this to a member of IT Support staff immediately.
- If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, the lesser the chances of your data being recoverable (mere minutes can count).

Reporting Breaches of this Policy

All members of staff have a duty to ensure this Acceptable Use Policy is followed. You must immediately inform a member of the IT Support staff, or the Headteacher, of abuse of any part of the computer system. In particular, you should report:

- any websites accessible from within Academy that you feel are unsuitable for staff or student consumption;
- any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc.;
- any breaches, or attempted breaches, of computer security; or
- any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the Academy computer system.

Reports should be made either via email or the Parago Helpdesk System. All reports will be treated confidentially.

Review and Evaluation

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.

Notes

"Sensitive personal information" is defined as information about an individual that is protected by law under the Data Protection Act 1998. Examples of such data include addresses and contact details of individuals, dates of birth, and pupil SEN data. This list is not exhaustive. Further information can be found in the Academy's Data Protection Policy.

Staff AUP Acceptance

I have read and understood the Parallel Learning Trust acceptable use policy for staff and agree to abide by its terms and conditions.

Name: _____

Signature: _____

Date: _____