Dane Court Grammar School
IT Systems Acceptable Use Policy – Students

Use of school computers and IT equipment by students 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 the school community should consider that the spirit of this policy applies whenever you are undertaking an activity that stems from your school related work. Use of the school network is intended to be as flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to limit the ways in which you can use the system, but to ensure compliance with the School's responsibilities to safeguard students and staff and protect the reputation of the School.

By using the school's IT and related systems you are agreeing to the terms of this acceptable use policy.

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.

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.
- Transmit any sensitive information or personal data relating to staff or students electronically without the data being encrypted by a method approved by the school.

You must:

- Ensure you have either logged your account off or locked the computer to prevent anyone using your account in your absence.
- Make your own backup of data kept on any storage system other than the school network storage drives "Shared Areas" or your 'My Documents' folder or Google Drive. This includes but is not limited to USB memory sticks (even those owned or issued by the school).
- 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.

Monitoring
The School's employs a number of systems to ensure computer systems are kept safe and used appropriately, including but not limited to:

- **Web Filtering;** This is used to protect all users from accessing inappropriate content from the School's network and can be used to review users internet activity in the event of concerns arising. Regular reports may be used to review internet usage and flag inappropriate usage.
- **Anti-Virus:** This software is also used to protect against the spread of viruses, spyware and malware and may also prevent access to malicious websites. The School's anti-virus is also used to block software and systems that may be harmful to the school network or may be used to circumvent the School's security systems. All alerts raised by the anti-virus software are flagged and monitored.
- **Impero Software:** This is a classroom management tool which is used to enhance teacher's ability to support student in their work. In addition it also provides real-time monitoring of appropriate computer usage in classrooms. The software may flag specific keywords for review and can automatically screenshot and/or record flagged content, and is actively monitored.

Use of Personal Devices
When using personal devices please ensure that any sensitive or personal information is secured to prohibit access by others. **You must not store school related data on personal devices without explicit permission.**

Equipment taken off-site
When our equipment is taken off site all precautions should be taken to prevent loss or damage. For example we would expect laptops to be locked in a car boot when the vehicle is unoccupied and kept out of sight when at home and not in use.

Personal Use
The school recognises that occasional personal use of the school's computers is beneficial both to the development of IT skills and 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 school policies;
- Must not interfere in any way with your work/studies;
- Must not have any undue effect on the performance of the computer system; and
- Must not be for any commercial purpose or gain.

Personal use is permitted at the discretion of the School and can be limited or revoked at any time. Please also be aware that personal usage may be monitored and flagged by the School's security systems.

Use of your own Equipment

- Any mains-operated 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. Tests must be performed at regular intervals as required by school's normal rules on electrical safety testing.
- You must not connect personal computer equipment to school computer systems without prior approval, with the exception of storage devices such as USB memory sticks.
- You must ensure that personal storage devices (such as a USB memory sticks) are kept virus and malware free, to protect the school's systems against the proliferation of harmful software

Conduct
You must conduct yourself appropriately at all times. This includes being polite and using the system in a safe, legal and 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, discriminatory 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 school's computer systems or when using your own devices.
You must make efforts not to intentionally waste resources. Examples of resource wastage include:

- Excessive downloading of material from the Internet;
- Excessive storage of unnecessary files on the network storage areas;

You must not eat or drink around computer equipment.

Confidentiality and Copyright

- You must respect the work and ownership rights of all people including people outside the school, as well as other staff or students.
- 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 school 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 to use the materials.
- By storing or creating any personal documents or files on the school computer system, you grant the school a non-exclusive, universal, perpetual, irrevocable, and royalty-free license to use, copy, and distribute those documents or files in any way the school sees fit.

Reporting Problems with the Computer System

It is the job of the Network Manager to ensure that the school 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 as soon as is feasible.
- If you suspect your computer has been affected by a virus or other malware, you must report this to a member of IT Services 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 less chances there are of your data being recoverable.

Reporting Breaches of this Policy

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

- Any websites accessible from within school 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.

Reports should be made either in person, via email or IT helpdesk at the earliest possible opportunity. All reports will be treated confidentially.

Review and Evaluation

This policy will be reviewed regularly. Changes to this policy will be communicated to all members of our community.

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 school's Data Protection Policy.