ACCEPTABLE USE POLICY - STAFF

Document Owner	**Head Master**
Author	**Head of Computing**
Date of Last Review	**November 2019**
Date of next review	**November 2022**

Acceptable Use of ICT Policy

1. Purpose

Pate's Grammar School actively promotes the responsible use of ICT to all users. When accessing the Pate's network (including using the remote access, CITRIX) users are agreeing to abide by the terms set out in this policy. The policy details the expectations of all users of ICT equipment and has been designed to work alongside and in conjunction with the school's Safeguarding, E-Safety, Whistleblowing and Data Protection Policies.

2. Scope

ICT as referenced in this document refers to all applicable ICT devices (whether personal or school owned) including but not limited to desktop PCs, laptops, mobile phones, tablet computers, portable storage and media whether connected or disconnected from the school's network. Authorised users are deemed to be any person who is issued with a user account or wireless connection details by the school.

This policy covers all individuals working at all levels and grades (collectively referred to as staff in this policy).Scope and purpose of the policy

This policy applies to all devices used to access our IT resources and communications systems (collectively referred to as systems in this policy), which may include (but are not limited to) smartphones, mobile or cellular phones, PDAs, tablets, and laptop or notebook computers. When you access our systems you may be able to access data about the School, including information which is confidential, proprietary or private (collectively referred to as school data in this policy).

When you access our systems using a device, we are exposed to a number of risks, including from the loss or theft of the device, the threat of malware and the loss or unauthorised alteration of school data. Such risks could result in damage to our systems, our business and our reputation.

Breach of this policy may lead to us revoking your access to our systems, whether through a device or otherwise. It may also result in disciplinary action up to and including dismissal.

3. Roles and Responsibilities

The Governing Body is responsible for ensuring that:

- The School's Responsible Use of ICT policy is maintained and updated regularly.
- That procedures and strategies related to the policy are implemented.
- Ensuring that all hardware and software are appropriately licensed for use.

The Head Master and Senior Leadership Team (SLT) are responsible for:

- Maintaining this policy, providing advice and guidance on its implementation.
- Ensuring that staff are aware of their responsibilities and are given relevant training and support.

The Director of eLearning is responsible for:

- The promotion of the Responsible Use of ICT equipment amongst staff and students.
- Providing training and support to enable users to use ICT equipment responsibly.
- Advise SLT on key aspects of Responsible Use and appropriate strategies to manage breaches.

The IT Services Manager and IT staff are responsible for:

- Security of the school information systems which will be reviewed regularly via the IT Services Manager.
- Monitoring the school's system and reporting breaches of the Responsible ICT Use Policy to the SLT.
- Advising and supporting the staff in dealing with Responsible ICT Use issues in the school.

The Communications Officer is responsible for:

- The promotion of responsible use of social media for the promotion and coordination of school activities.
- Monitoring school owned social media.

All staff have a responsibility for:

- Ensuring responsible ICT use amongst student users.
- Demonstrating best practice.
- Dealing with incidents of breaches in the Responsible Use of ICT Policy.
- Reporting incidents of breaches in the Responsible Use of ICT policy within the school.
- Educating students about the responsible use of ICT.
- Engaging in training events on responsible use of ICT.
- Recording any serious incident in the E-Safety Incident Book, held with the Head's PA

All students are responsible for:

- Behaving in a way that does not breach the Responsible Use of ICT policy.
- Promoting the responsible use of ICT amongst their peers by adopting best practice.

Visitors must:

- Sign in on arrival and out on departure at the School Office and by signing in:
  - Have read the summary of the Safeguarding procedures on arrival at the School.
  - Accept the Responsible Use of ICT Policy.
  - Follow the instructions of staff when on site or accessing the school's IT system.

4. Principles

4.1 Access

Pate's Grammar School's ICT systems may be used by authorised users for any legal activity that is in furtherance of the aims and policies of Pate's Grammar School subject to the conditions below. Moderate use of the ICT systems for personal purposes will be permitted provided such activities take place outside of the normal times of educational use (defined in this context as running from 8.30 a.m. to 1.10pm and 2.10pm to 3.35pm during term time) and do not otherwise contravene the terms of this policy.

ICT systems should only be accessed via the authorised account and password provided by the IT Services team to individual users. Users may not make these details available to any other person; users will be held responsible for any breach of this policy performed through their account. If you believe that your password has been compromised, you should change it immediately and inform the IT Services staff.

Staff should not attempt to bypass any security systems put in place by the school. Any suspected damage to the school network should be reported immediately to the IT services manager.

Staff should ensure that any school devices taken off site (such as, but not limited to, pool laptops and cameras) are held securely, that devices are not stored overnight in a car or left in sight when not in use. Any loss should immediately be reported to the IT services manager.

Connecting devices to our systems

Connectivity of all devices is centrally managed by the IT Manager, who must approve a device before it can be connected to our systems. We reserve the right to refuse or remove permission for your device to connect with our systems.

In order to access our systems it may be necessary for the IT Department to install software applications on your device. If you remove any such software, your access to our systems will be disabled.

4.2 Data and Communications

All communications and information stored on the ICT systems should be assumed to be property of Pate's Grammar School. Any items stored in your user area or folders within your user area maybe subject to deletion. No member of Pate's Grammar School including the Head Master or the governors can't be held responsible for any loss of data.

All portable storage media must be checked for viruses prior to use. Suitable encryption should be used to ensure compliance with the Data Protection Policy. See the IT Services team for guidance.

Users are provided with their own email account for educational use only. Personal use of email accounts (for emailing friends in school etc.) is not permitted as this uses up valuable network bandwidth and storage space that could be better used elsewhere.

Users are responsible for the content of all emails sent and received by them. The sending of offensive, profane or abusive email or other messages is forbidden. If users receive any offensive or inappropriate emails they should report it to the IT Services Office immediately. Use of school email accounts for bullying or harassment will not be tolerated. Email attachments should only be opened if they come from a known and trusted source. The sending of email attachments containing any program, file or shortcut that damages or shuts down a computer, damages or alters the operating system or alters, deletes or otherwise modifies user files is strictly forbidden.

The use of email rules that disrupt, slow down or damage the school mail server or network system is not permitted.

- Emails to students should be restricted to matters of formal communication from Pate's Grammar School, e.g. school trips, school work, pastoral matters etc.
- Communication must only be sent through Pate's Grammar School's email systems; staff must not communicate with students via their personal email accounts.
- The use of personal ICT equipment to access school email is permitted. Users should set a strong password on their device and report lost or stolen devices that connect to the school network to IT Services immediately and Pate's reserves the right to inspect e-mails when directed by Governors or SLT.
- SMS (texting) must NOT be used for formal or personal communication to students. In the case of field trips, DofE, use of a school mobile phone is acceptable for emergency SMS communication as is communication to a TA with accessibility issues.

4.3 Social Media (defined in Appendix 3)

The school utilises social media in an official capacity as a marketing and communication tool.If an Internet post would breach any of our policies in another forum, it will also breach them in an online forum. All school social media accounts must provide full transparency to the Head Master, SLT and Governors:

Acceptable Use of ICT Policy

School Owned Accounts

- Must have a connection with administrative privileges to the main school accounts which are controlled by the Communications Officer.
- Where social media is being used for communication with students it should be a closed group (secret group) where membership is by invitation by staff only.
- Students must not be given administrative privileges for any school account.

Staff Personal Social Media Accounts

We recognise that staff may work long hours and occasionally may desire to use social media for personal activities at the office or by means of our computers, networks and other IT resources and communications systems. We authorise such occasional use so long as it does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity. While using social media at work, circulating chain letters or other spam is never permitted. Circulating or posting commercial, personal, religious or political solicitations, or promotion of outside organisations unrelated to the organisation's business are also prohibited. Staff must ensure that their use of social media does not create any breaches of internet security and therefore must be careful to avoid any applications that might interrupt our IT systems. Excessive use of social media that interrupts staff productivity will be subject to a disciplinary procedure, consistent with this policy.

Key points of conduct:

- When logging on to and using social media websites and blogs at any time, including personal use on non-school computers outside the workplace and outside normal working hours
- ensure that wherever possible their privacy settings on social media sites are set so that pupils cannot access information relating to their personal lives;
- obtain the prior written approval of the Head Master, to the wording of any personal profile which you intend to create where the School is named or mentioned on a social networking site;
- seek approval from the Head Master before they speak about or make any comments on behalf of the School on the internet or through any social networking site;
- report to a member of SLT immediately if they see any information on the internet or on social networking sites that disparages or reflects poorly on the School;
- immediately remove any internet postings which are deemed by the School to constitute a breach of this or any other School policy;
- weigh whether a particular posting puts their effectiveness as a teacher at risk;
- post only what they want the world to see.

Acceptable Use of ICT Policy

Staff must not

- Other than in relation to the school's own social media activities, write about their work for the school.
- Conduct themselves in a way that is potentially detrimental to the school or brings the school or its students, employees, clients, customers, contractors or suppliers into disrepute, for example by posting images or video clips that are inappropriate or links to inappropriate website content.
- Allow their interaction on these websites or blogs to damage working relationships with or between employees and clients, customers, contractors or suppliers of the school, for example by criticising or arguing with such persons.
- Include personal information or data about the school's staff, students, customers, contractors or suppliers without their express consent.
- Make any derogatory, offensive, discriminatory, untrue, negative, critical or defamatory comments about the school, its employees, students, clients, customers, contractors or suppliers.
- Make any comments about the school's employees that could constitute unlawful discrimination, harassment or cyber-bullying contrary to the Equality Act 2010 or post any images or video clips that are discriminatory or which may constitute unlawful harassment or cyber-bullying - employees can be personally liable for their actions under the legislation.
- Disclose any trade secrets or confidential, proprietary or sensitive information belonging to the school, its employees, students, clients, customers, contractors or suppliers.
- Use personal social media for communication with any current students or former students under the age of 18.
- Access personal social networking sites during school hours.
- We prohibit staff from using their work email address for any personal use of social media
- provide references for other individuals, on social or professional networking sites, as such references whether positive or negative can be attributed to the School and create legal liability for both the author of the reference and the School;

The monitoring of social media

The contents of our IT resources and communications systems are School property. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings, email and web activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

We may store copies of such data or communications for a period of time after they are

created, and may delete such copies from time to time without notice.

Do not use our IT resources and communications systems for any matter that you wish to be kept private or confidential from the organisation.

Social media and the end of employment

If a member of staff's employment with our School should end, for whatever reason, any personal profiles on social networking sites should be immediately amended to reflect the fact that you are no longer employed or associated with our School.

All professional contacts that a member of staff has made through their course of employment with us belong to our School, regardless of whether or not the member of staff has made social media connections with them.

4.4 Internet Access

You must not visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Pornography.
- Promoting discrimination of any kind.
- Promoting political extremism
- Promoting racial or religious hatred.
- Promoting dangerous or illegal acts.
- Hacking, proxies or any other method of bypassing network security.
- Any other information which may be offensive, slanderous or seen as a form of bullying to other students or employees of Pate's Grammar School.
- That might be defamatory or incur liability on the part of Pate's Grammar School or adversely impact on the image of Pate's Grammar School.

You must not:

- Download any screensavers, wallpapers, games or any other programs. These may contain viruses and the process of downloading uses excessive Internet bandwidth.
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate.
- Subscribe to any mailing lists; make use of chat lines, forums or messaging services.

4.5 Core Values

The following values contribute to the responsible use of ICT facilities:

Users must not:

- Damage or waste any ICT equipment or supplies.
- Consume food or drink of ANY description in the ICT rooms including chewing gum.
- Copy programs to or from the school network (or any computer attached to it).
- Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the network.
- Attempt to bypass network security in anyway including, but not limited to, the use of proxy sites.
- Carry out bulk emailing or forward “chain mail”.
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties.
- Use the ICT facilities for running a private business.
- Enter into any personal or financial transaction.
- Reveal or publicise confidential or proprietary information, which includes but is not limited to: financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships.
- Create, propagate or publish any inappropriate or offensive information or media about or featuring Pate’s Grammar School, its students or its employees, this includes but is not limited to:

    - Use personal ICT equipment to take pictures and videos in and out of the classroom without the direct supervision of a member of staff.
    - Distribute pictures, videos via Bluetooth, infrared, MMS or any other mobile technology.
    - Upload of videos onto video sharing sites including but not limited to You Tube.
    - Upload of pictures onto picture sharing sites including but not limited to Flickr.
    - Post comments on social networking sites including but not limited to Facebook and Twitter.

4.6 Personal Devices

- This policy applies to any device that you may bring on to school premises and you are expected to abide by this policy when accessing the internet or network through any device.
- Students may not use personal ICT devices in lessons unless it is being used as part of the lesson or with the express permission of the supervising teacher.
- The school holds no responsibility for the safe keeping or functionality of personal ICT devices.

Security requirements

You must comply with the Use of Phone, E-Mail systems and Internet Policy in our Staff Handbook when using your device to connect to our systems.

We reserve the right, without further notice or permission, to inspect your device and access data and applications on it, and remotely review, copy, disclose, wipe or otherwise use some or all of the school data on it for legitimate business purposes.

You must co-operate with us to enable such inspection, access and review, including providing any passwords or pin numbers necessary to access the device or relevant applications.

If we discover or reasonably suspect that there has been a breach of this policy, including any of the security requirements listed above, we shall immediately remove access to our systems and, where appropriate, remove any school data from the device. Although we do not intend to wipe other data that is personal in nature (such as photographs or personal files or e-mails), it may not be

possible to distinguish all such information from school data in all circumstances. You should therefore regularly backup any personal data contained on the device.

Lost or stolen devices and unauthorised access

In the event of a lost or stolen device, or where a staff member believes that a device may have been accessed by an unauthorised person or otherwise compromised, the staff member must report the incident to the IT Manager immediately.

Appropriate steps will be taken to ensure that school data on or accessible from the device is secured, including remote wiping of the device where appropriate. The remote wipe will destroy all data on the device (including information contained in a work e-mail account, even if such e-mails are personal in nature).

Although we do not intend to wipe other data that is strictly personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from school data. You should therefore regularly backup all personal data stored on the device.

Procedure on termination of employment

On your last day of work, or your last day before commencing a period of garden leave, all school data (including work e-mails), and any software applications provided by us for work purposes, will be removed from the device. If this cannot be achieved remotely, the device must be submitted to the IT Manager for wiping and software removal. You must provide all necessary co-operation and assistance in relation to this process.

4.7 Copyright & Licensing

Virtually all commercial software is subject to copyright as well as licensing laws. The use of the ICT Systems for making copies of software (other than for legitimate back-up purposes) is prohibited. No images, videos or audio that is in breach of copyright restrictions should be downloaded

5. Links to other Policies

Anti-bullying Policy
Data Protection Policy
E-Safety Policy
General Complaints Policy
Safeguarding Policy
Whistleblowing Policy

The Governors of Pate's Grammar School reserve the right to amend this policy at any time. Such changes will become effective upon posting of the updated policy.

Acceptable Use of ICT Policy

Appendix 1 to the Responsible Use of ICT Policy

General Advice

- Be careful with your personal details on the Internet especially on social networking sites such as Facebook and chat rooms.
- Backup your work, the school cannot be held responsible for any loss of data.
- Please report all damage and/or faults of school owned ICT to the IT Services Team.
- Please report anything that you think maybe in breach of this policy to the IT Services Team
- Printing is a costly process and has environmental impact – please think before you print.
- You MUST keep your password a secret, and immediately change it if you feel it has become known
- Save pictures as .jpg format, DO NOT save as .BMP (too large).
- Do not logon with another person's details
- If you have a social networking profile you should:
  - Ensure your profile is private
  - Consider what photos are accessible on your profile and how this may reflect on you in school.
  - Consider what you write on your profile and how this may reflect on you in school.
  - Deny links to students of Pate's Grammar School
  - Give careful consideration to any access by former students who may have links to current students

Acceptable Use of ICT Policy

Appendix 2 to the Responsible Use of ICT Policy

Response to Misuse

Failure to comply with this policy may lead to the school taking any one or more of the following actions:

All Users

- Any illegal activity will be reported to the police.

Staff

- The issue of a verbal warning.
- The issue of a written warning.
- The suspension of a user's account.

or in serious cases:

- The termination of a user's account.
- The commencement of formal disciplinary proceedings.
- Taking legal action.

Students

- Inappropriate use of the Internet may result in restriction of some or all internet or IT access
- All other sanctions will be in line with the Behavior Policy
- Serious offences will be reported to the Senior Leadership team and may result in a fixed term or permanent exclusion.

Visitors

- Devices will be blocked from connectivity and accounts deactivated

Acceptable Use of ICT Policy

Appendix 3 to the Responsible Use of ICT Policy

Social Media

Social media is an interactive online media that allows users to communicate instantly with each other or to share data in a public forum. It includes social and business networking websites such as, but not limited to, Facebook, Twitter and LinkedIn. Social media also covers video and image sharing websites such as, but not limited to, YouTube and Flickr, as well as personal blogs. This is a constantly changing area with new websites being launched on a regular basis and therefore this list is not exhaustive. This policy applies in relation to any social media that may be used.

The School recognises that many employees make use of social media in a personal capacity outside the workplace and outside normal working hours. While they are not acting on behalf of the school in these circumstances, employees must be aware that they can still cause damage to the school if they are recognised online as being one of its employees. Therefore, it is important that the school has strict social media rules in place to protect its position.