Woodlands

respect resilience responsibility

ICT Acceptable Use & E-Safety Policy

Date:	September 2018
Review Date:	July 2019

Woodlands ICT Vision

Our vision is that ICT should be

Accessible to all,

Sustainable,

Safe and secure,

Fast and effective,

and that it must

Enhance learning,

Raise standards,

Empower,

Inspire,

Promote community cohesion

&

Facilitate lifelong personalised learning

Table of Contents

Rationale

This policy document outlines the schools' technology systems and what is deemed as acceptable usage of these systems. The school uses a range technology based systems to assist it in smooth running of the school.
These technologies encourage the development of communication skills and transform the learning process by opening up possibilities that, conventionally, would be impossible to achieve.

The school encourages the use of electronic mail (e-mail) as a medium for paper mail replacement in order enhance communications and apply its commitment to reduce its carbon footprint.

The school does however recognise the dangers that these technologies can also generate.

This policy sets out the expectations of staff, students and other users (working for or on behalf of Woodlands Community College).

This policy applies to all Internet, Intranet, e-mail, messaging systems and all related technology services and equipment provided by the School, and to all users accessing these services.

This policy is designed to express Woodlands' philosophy with regard to the Internet, Intranet and electronic communication in general and to set forth general principles users should apply when using these services at the school site, when working from remote locations, when using the schools' name or when using resources provided by the school. This guidance does not attempt to cover every possible situation.

In order to make the policy as easy to follow as possible it has been broken down into three sections:

- Staff Acceptable Use Policy (SAUP)
- Student Acceptable Use Policy
- Parental Guidance and Agreement (PGA)

The rationale and introduction sections are relevant to all stakeholders. Students and parents can then jump to the appropriate section if they wish. Staff should read the policy in its entirety to ensure that they are familiar with the student acceptable use.

If you are viewing this document electronically there are also hyperlinks throughout to help you jump to the relevant sections, including directly from the Table of Contents Page.

Each section includes school policy, procedures, advice, guidance and general information.

The policy does not attempt to cover every possible scenario that may arise.

If a user is in doubt of whether an action may contravene policy then they should raise the concern with a member of staff listed on the key contacts page.

Introduction

The school believes that the creation of a safe ICT learning environment includes three main elements at the School:

1. An effective range of technological tools;
2. Policies and procedures, with clear roles and responsibilities;
3. Access to E-Safety information for students, staff, parents, carers and other users.

The school provides its staff and students with a multitude of tools, including the following:

Hardware	Software	Web associated technologies
Laptops	Microsoft Office 2010, 2013, 2016	Onsite filtered usage of the Internet
PC's	Windows Operating System – XP, 7 & 10	Maths Watch VLE
Apple Mac's	Mac OS Operating System	Lexia Reading
Radio Studio	Windows Server 2008 & 2012	Accelerated Reader
Wireless access points	Eclipse.Net & MLS Connect Library software	Google Apps for Education (Email, Online Storage, Classroom, Calendar, Google Sites)
Printers	Sims InTouch	Official Facebook Page
Network Switches	Impero Network Management	Official Twitter Page
iPads	Livedrive backup	Sumdog Maths Activities
Interactive Whiteboards	Promethean Activ Inspire & Studio	Manga High Maths Activities
Projectors	Starboard	Doddle Science Platform
Digital Cameras	Eclipse.Net & MLS Connect Library software	Sharp System – Report Concerns
Sound output equipment	Capita Sims.Net	My Maths
Sound recording equipment	Comic Life Studio	SISRA Online and Analytics
Scanners	Visit-ED	CPOMS
CCTV	Papercut	Lexia Core 5 & Lexia Reader
	Logit Lab	Sims Parent App
	Lucid LASS	
	Lucid Memory Booster	
	Lucid Exact	
	Techsoft 2d Design & 2D Design V2	
	Exam Wizard PE	
	PCD Wizard	
	Livewire	
	Python	
	Pygame	
	Control Studio	
	Serif Media Suite – photo editor, web designer, video studio	
	Microsoft Security Essentials	
	Fortinet VPN SSL Client	

This policy is also inherently linked to the Data Protection Policy, Safeguarding Policy, Anti-Radicalisation Policy and Behaviour for Learning Policy; available from the Policies section of the school website - http://www.woodlands.southampton.sch.uk/parental-info/policies/.

The school also follows the DfE guidance on Keeping Children Safe in Education 2018, which can be viewed/downloaded by clicking visiting:
https://tinyurl.com/y8du3kt4.

Staff E-Safety Guidance

The school delivers an annual safeguarding training session to staff each September, which includes e-safety guidance, and outlines that safeguarding is the responsibility of every single member of staff.
New members of staff receive this training as part of their induction programme upon joining the school.
Attendance to the delivery of these training sessions are recorded and stored centrally.
As part of the Safeguarding Training, staff are advised who how to log safeguarding concerns electronically, and who the schools' Designated Safeguarding Leads (DSL) are. This policy also highlights key personnel with regards to e-safety on the Key Contacts Page.

Every member of staff will also be expected to complete the PREVENT/Channel training in order to ensure that they are fully aware of:

- the threats, risks and vulnerabilities that are linked to radicalisation
- are aware of the process of radicalisation and how this might be identified early on
- are aware of how the school can provide support to ensure that our students are resilient and able to resist involvement in radical or extreme activities.

Students E-Safety Guidance

Students are regularly taught about how to stay safe when using electronic media through the ICT curriculum, assemblies and the school PD programme, which includes workshops and presentations from external agencies.

One of the key messages which is delivered to students, is to recognise that people are not always who they say they are online.
Students are also taught how to seek adult help if they are upset or concerned about anything they read or see or to use the CEOP button, located on the Safeguarding page of the school website as and when appropriate.
The school has also invested in a piece of online software called the Sharp System. This system can be used by students to report concerns over bullying. The site also includes information on bullying, weapons, health and hate crimes. This can be accessed via the students intranet homepage from a school device or from outside of the school by navigating directly to the url - http://woodlands.thesharpsystem.com/index.php.

In addition, parents and all stakeholders can also keep closely in touch with safeguarding guidance and via the safeguarding and e-safety page on the school website http://www.woodlands.southampton.sch.uk/safeguarding-e-safety/ which includes a live feed of e-safety news and resources by the PARENTINFO service from CEOP and Parent Zone organisations.

Staff Acceptable Usage Policy (SAUP)

This section of the policy focuses its aim at Staff providing:

- acceptable usage information including restrictions placed upon users, equipment and the school reputation;
- guidelines on usage;
- guidance on E-Safety
- guidance on data protection.

It does not attempt to cover every possible scenario that may arise.

Defining Unacceptable Use

The Internet, Intranet, email, messaging systems and related technologies must not be used for knowingly viewing, transmitting, retrieving, downloading, printing or storing any communication or material that is:

- Discriminatory or harassing;
- Derogatory to any individual or group;
- Obscene or pornographic;
- Defamatory, threatening or seen as cyber bullying;
- Illegal or contrary to school policies or interests;
- Subject to copyright restrictions such as music, books or extracts, software or films;
- Likely to cause network congestion or significantly hamper access for other users;

With the exception of being the recipient of any such material, in which case; users should notify IT Support or their line manager.

Staff should also be conscious that uploading any of the above categories into the public domain may result in disciplinary action.

Law and this policy prohibit the theft or abuse of computing resources including:

- Unauthorised entry;
- Using, transferring and tampering with user accounts and files not specifically belonging to themselves;
- Interfering with other people's work or computing facilities;
- Sending, storing or printing offensive or obscene material including content that may be interpreted as sexual or racial harassment;
- Mass mailing of messages – chain and spam;
- Internet use for personal commercial purposes;
- Using the internet/intranet facilities or equipment to deliberately propagate any virus, worm, trojan horse or any such other programme that is harmful to normal computer operations;
- Accessing or uploading to any obscene or pornographic sites or material. Sexually explicit material may not be viewed, archived, stored, distributed, edited or recorded using the School's networks or computing resources.

If a user finds themselves accidentally connected to a site or program that contains sexually explicit or offensive material, they must disconnect from that site immediately. Such unintentional access to inappropriate internet sites must be reported immediately to the respective line manager and where necessary to The Head Teacher, and Designated Safeguarding Lead. Any failure to report such access may result in disciplinary action.

It is impossible to define all possible unauthorised use, however, disciplinary action may be taken where a user's actions warrants it. Other actions deemed unacceptable, although not exhaustive, include:

- Theft or copying of files without permission;
- Sending or posting the Schools' or Local Authority's confidential files outside of the organisation or inside the organisation to unauthorised staff, students or other users;
- Refusing to co-operate with reasonable security investigation;

Using Email, Messaging and Social Networking systems

Each member of staff will be provided with a school email account, so as to enhance communication.
Staff are expected to use their email facility responsibly, comply with all applicable laws, other policies and procedures of the School, and with normal standards of professional and personal courtesy and conduct.
Appendix 4 provides an illustration of good practice.

Email Guidelines

In order to effectively manage email systems, following should be adhered to:

- All emails sent by staff must include a subject that needs to be as specific as possible
- If the email is of a short nature then then "EOM" must be added at the end of the subject line to indicate "End Of Message". This is to reduce the amount of emails that need to be opened by staff, thereby reducing workload
- Care should be taken about the content of a message as it has the same standing as a letter therefore all emails written to students, parents, or external agencies should be professional in manner
- Emails to students and parents are encouraged as long as they adhere to school policy and the content is professional. However, emails must only be sent using the school email system and not any personal system belonging to any member of staff.
- To enhance the opportunities to communicate via email all letters sent from the school must include the email address of the sender. Parents must also be offered the opportunity to communicate via email as an alternative method of communication in all verbal conversations.
- Staff must use the sent box facility of their email as a record of correspondence and must not, therefore, delete items from this. Users can archive sent items by exporting the Sent items to a Outlook PST file if their mailbox size is becoming too large.
- When filling a student behaviour log on Sims, if an email has been sent, it is good practice to record this communication from the available options.
- Report any inappropriate email use to IT Support Desk – e.g. phishing attempts, breaches of security or suspected virus
- It is recommended that users are very cautious when opening any email that appears in "Junk E-mail" when accessing through Outlook; or "Spam" when accessing via the Google web interface
- When sending email, staff should consider carefully who needs to receive email, and make use of the appropriate distribution lists ie teaching_staff@woodlands.southampton.sch.uk for teaching staff or partnership_staff@woodlands.southampton.sch.uk for partnership staff. This will avoid staff accounts being flooded with unnecessary messages.

Staff email users must not do any of the following:

- Ignore messages. These systems are designed for speedy communication. If the message requires a reply, a response should be sent as promptly as possible, but no later than within 48 hours (working day 8am to 4pm) of receipt
- Abuse others, even in response to abuse directed at them
- Use these technologies, either internally or on the Internet, to harass or threaten anyone in any manner
- Forward chain mail

When using the school email system, staff should consider that any comment that they make using the system may get forwarded on as part of a conversation between other people. It is therefore important that staff ensure that the use of the email system is done so in an appropriate and professional manner.

Email signature blocks are be setup automatically for staff to give a formal standardised approach to all dialogue. Staff should also ensure that spelling and grammar checks are done prior to sending email and that there is no profound language used throughout.

Woodlands Community College encourages a work life balance. Therefore, staff are encouraged not to send emails during school holidays or weekends.

Using school equipment/services outside of work

Users accessing the Internet from home or in a public place whilst using equipment provided by the school or to access connections into the school must adhere to the policies set out in this document.

Users must not grant unauthorised access to the school network or any school information resources under the GDPR. Usage of school computer equipment may be granted when supervised by school staff to ensure that the restrictions outlined by this policy are adhered to.

Personal use of school equipment/services

The Internet, Intranet, e-mail, messaging systems and other related technologies are business tools provided to users at significant cost. Hence, it is expected that this resource will be used primarily for business related purposes. Reasonable access and use of these systems is also available to recognised representatives of professional associations i.e. Union Officers.

These systems may be used for incidental personal purposes, provided that it does not:

- Contravene the statements laid out in the misuse section
- Interfere with the schools' operation of computing facilities or e-mail services
- Interfere with the user's employment or other obligations to the school
- Interfere with the performance of professional duties
- Is of a reasonable duration and frequency
- Is performed in non-work time
- Does not over burden the system or create any additional expense to the school or workload to staff

All such use should be done in a manner that does not negatively affect the use of the schools' systems for business purposes. Users are expected to demonstrate a sense of responsibility and not abuse this privilege.

Privacy of information stored on/transmitted by Woodlands equipment

Data Protection

The School is obliged to take proper care of the information that it holds, processes and uses to deliver services, particularly where that information contains personal or sensitive personal details, or is of a confidential nature.
The GDPR/Data Protection Policy tells users what their responsibilities are for protecting the information that they use to do their jobs.

The School follows sound professional practices to secure e-mail records, messaging systems, data and system programmes under its control. As with standard paper based mail systems, confidentiality of these cannot be 100% assured. Consequently users should consider the risks when transmitting highly confidential or sensitive information and use the appropriate level of security measure.

Enhancement of the base level security to a higher or intermediate level can be achieved by the use of passwords to encrypt confidential files.
It should be remembered messages forwarded from another individual can be amended by the forwarder. This possibility should be considered before acting on any such mail.

In order to effectively manage these systems, the following should be adhered to:

- Open messages/mailboxes must not be left unattended or displayed using a projector
- Transmit usernames and password without appropriate encryption
- Send personal data that would be categorised as sensitive under the GDPR.
  CPOMS should be used as a platform to communicate sensitive information about students/young people amongst internal users.
  If the information is to be communicated to an external agency then the sensitive information should be encrypted and sent as an attachment, with the password sent in a separate medium of communication i.e. phone call.

Privacy

Woodlands respects users' privacy, and therefore e-mail content will not be routinely inspected, however the school does reserve the right to intercept and monitor where it sees fit to do so.
Inspection and interception may be triggered as a result of the following:

- When required by law
- If there is a substantiated reason to believe that a breach of any school policy has taken place
- When there are emergency or compelling circumstances

The School reserves the right, at its discretion, to review any user's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other policies.

Users should not have any expectation of privacy to his or her internet usage. The School reserves the right to inspect any and all files stored in computers or on the network in order to assure compliance with this policy. Auditors must be given the right of access to any document, information or explanation that they require.

The use of staff designated personal file area on the network server provides some level of privacy in that it is not readily accessible by other users. These file areas will however be monitored to ensure adherence to the School policies and to the law. The user's personal file area (S: Drive) is disk space on the central server and is allocated to that particular user.

Managers will not routinely have access to a user's personal file area. However, usage statistics/management information on usage size of drives or a report outlining the amount of information held on an individual's personal file area will be made available if necessary.

Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership, with the support of Governors, aims to embed safe practices into our culture. A member of the Senior Leadership Team shall ensure that the Policy is implemented and that associated monitoring is effectively carried out. The responsibility for E-Safety curriculum has been designated to the lead teacher for Digital Learning. The referrals regarding e-safety concerns should be logged in CPOMS and these will be actioned through the fortnightly safeguarding meeting.

A list of key contacts and their roles can be found at the Key Contacts section in this document.

The schools' E-Safety Co-ordinator ensures they keep up to date with E-Safety issues and guidance through liaison with the Local Authority, the DfE and through organisations such as The Child Exploitation and Online Protection service (CEOP). The School E-Safety Co-ordinator ensures that the School Senior Leadership Team and/or Governors are updated as necessary and that other appropriate members of staff are also updated e.g. Pastoral Team and IT Support Staff.

Governors need to have an overview understanding of E-Safety issues and strategies. Where appropriate, the school will ensure Governors are aware of our local and national guidance on E-Safety and are updated annually on policy developments.

All staff are responsible for promoting and supporting safe behaviours in their classrooms and following E-Safety procedures.

All staff should be familiar with this policy including:

- E-mail, messaging and digital communication (social networking) use
- Safe use of the school network, equipment and data
- Safe use of digital images and digital technologies, such as digital cameras and video cameras
- Publication of student information/photographs and use of the Intranet, school website, School Facebook Page, School Twitter feed, School newsletter and any other generated literature as per the GDPR/Data Protection Policy and Safeguarding Policy.
  Sadye Sydenham holds the consent register for publication of names and photographs and internet access. Staff should ensure that they check with Sadye before publicising names or photographs of any student, that parental permission has been granted following the completion of Web Publication of Work and Photographs Consent section on the student registration form.
- E-Bullying/cyber-bullying procedures as per the Behaviour for Learning Policy
- Their role in providing/accessing E-Safety information

Staff and students are reminded about E-Safety matters and amendments to the policy are drawn to staff attention by the E-Safety Co-ordinator as they occur.

Reporting student E-Safety concerns

Woodlands operate all recording of safeguarding concerns using an online tool called CPOMS (Child Protection Online Monitoring System).

All staff have been issued personal login information to access the site and receive training on how to use the site from the school DSL.
Where staff have an E-Safety concern for a student, they should report their concern immediately via CPOMS. This will alert key members of staff so that the matter can be investigated immediately. Staff should try to ensure that as much information is provided as possible.

The role of the E-Safety Co-ordinator

In cases where a student is found to have participated in a seriously breach of this policy, the E-Safety Co-ordinator will request that IT Technical Support staff revoke the student's access to the school network and subsequent internet services until contact has been made with parents/carers. The E-Safety Co-ordinator will then explain the policy to parents and the student and the contract will be re-signed by both parties. Any associated cost may be passed onto the parent, as per point "h" in the Charging Policy.

The E-Safety Co-ordinator will track E-Safety incidents logged via CPOMS, and action them according to the schools' safeguarding policy. Where applicable the E-Safety Co-ordinator may also inform IT Support who may be able to provide extra evidence to support any case as well as make appropriate adjustments to the network and internet content filtering.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is taking place. This does not contradict the school's privacy policy as set out under the GDPR.

Social Networking guidelines to staff

The purpose of this section is to set out the School's recommendations and requirements for the use of social networking media by its employees. In doing so, the School seeks to achieve an appropriate balance in the use of social networks by staff as private individuals, but also as employees and educators, with professional reputations and careers to maintain, and contractual and legislative requirements to adhere to.

Whilst the School does not wish to discourage staff from using such sites on the Internet in their personal time, it does expect certain standards of conduct to be observed in order to protect the School and its reputation, and also to protect staff from the dangers of inappropriate use.

Accessing social networking sites in working time and/or from School ICT equipment is prohibited, whether the equipment is used at home or at school, with exception to the usage of the school social networking accounts. Therefore, this section largely relates to the use of social networking applications by School staff in their own personal time.

The term 'staff' covers all employees/staff of the School, including casual staff and agency employees. Where individuals from partner organisations are involved in acting on behalf of the School, they will also be expected to comply with this Policy.

Examples of social networking applications include, but are not limited to:

- Social Networking (e.g. Facebook, MySpace, Bebo)
- Media sharing services, (e.g. YouTube, Instagram, Periscope, WhatsApp, Snapchat)
- Micro-blogging applications (e.g. Twitter, Yammer)
- Online discussion forums and opinion sites (e.g. Ning)
- Blogs (e.g. Blogger, LiveJournal, Xanga)

Staff should:

- ensure that they are familiar with the contents of this policy and its relationship to the School's standards, policies and guidance on the use of ICT.
- raise any queries or areas of concern they have relating to the use of social networking sites and interpretation of this Policy, with their line manager in the first instance.
- comply with this policy where specific activities/conduct are prohibited.

Working in an educational setting with young people, means that staff have a professional image to uphold. Therefore, the way that individuals conduct themselves online, helps to determine this image.

Staff must not interact with students of the school, via any personal social media or electronic messaging account. The only exception to this rule would be that the member of staff is a family member to a member of staff. If staff are in any doubt over any contact that they may have with a student via social media/messaging then they should raise it with a member of the SLT.

Content of interactions using digital systems:

Staff are recommended to refrain from making reference on social networking sites to the School, its employees, students, and their families. If staff adhere to this recommendation, then the personal content of an individual's social networking memberships is unlikely to be of concern to the School.

An exception to the above would be content which details conduct outside of employment which affects the individual's suitability to perform his/her work, makes him/her liable to be unacceptable to other staff or management, or is liable to damage the School's reputation.

If employment at the School is referred to, then the information posted would need to comply with the conditions set out below:

- Any references made to the School, its employees, students and their families, should comply with the School's policies on conduct/misconduct, equal opportunities, bullying and harassment.
- Staff must not post information on a social networking site which is confidential to the School, its employees, its students or their families.
- Staff must not post entries onto social networking sites which are derogatory, defamatory, discriminatory or offensive in any way, or which have the potential to bring the School into disrepute.
- Staff should not use the School logo on their own personal social networking accounts, and should not post any photographic images that include students, except for when using the school's official social networking accounts.
- When posting any information onto a social networking site, staff are recommended to consider whether any entry they make puts their effectiveness to perform their normal duties at risk.
- If individuals feel aggrieved about some aspect of their work or employment, there are appropriate informal and formal avenues, internally within the School, which allow staff to raise and progress such matters. Social networks are not the appropriate forum to raise such matters. Employees should discuss any concerns with the Head Teacher/Line Manager in the first instance. Guidance is also available from HR/Payroll and trade unions.

Where staff use educational/professional networking sites as a professional resource, which are not available to the general public; it is acceptable to make reference to the school. The above conditions relating to content of postings/communications will still apply.

Security of profiles on social media

Staff are advised to check their security profiles and privacy settings on the social networks that they use. If individuals are not clear about how to restrict access to their content, they should regard all content as publicly available and act accordingly.

In using social networking sites, staff are recommended to only post content that they would wish to be in the public domain. Even if content is subsequently removed from a site it may remain available and accessible. Staff should consider not only how content could reflect on them, but also on their professionalism and the reputation of the School as their employer.

Even with privacy settings in place it is still possible that the personal details of staff may be accessed more broadly than the other networkers identified by them. Any reference to such information by students and/or their families, which a staff member deems to be inappropriate or is concerned about, should be reported to their line manager in the first instance.

If a member of staff becomes aware that a student (or group of students) has made inappropriate/insulting/threatening comments about them, or other staff members, on a social networking site; then they must report this to the Head Teacher so that the appropriate process can be followed.

Policy Breaches:

Staff found to be in breach of this policy may be subject to disciplinary action, in accordance with the School's Disciplinary Policy & Procedure and the Code of Conduct and Disciplinary Rules, with potential sanctions up to and including dismissal.

Information shared through social networking sites, even on private spaces, is subject to copyright, data protection, freedom of information, equality, safeguarding and other legislation.

Where staff work in roles that are governed by professional bodies/professional codes of conduct; the professional rules relating to social networking applied to them may be more stringent that those within this Policy.

IT equipment - general use guidelines

Data Protection

Staff should ensure that they are protecting the integrity of data held by the school by ensuring that any sensitive data is kept on local hard drives is in an encrypted container. If this data is transferred it should only be to authorised personnel and should remain encrypted during the transfer of the information.
Decryption instructions should be provided in an alternative way i.e. phone call. Inline with our GDPR compliance Woodlands has responsibility as a data controller to ensure that processors are also aware of their GDPR obligations. It is therefore good practice to advise the recipient that the data should be stored in an encrypted system whilst in their possession and check for their retention and erasure policies.

Security Updates

Users should ensure that the PC that they are assigned/using is fully restarted at least once every 24 hours. This is to enable security updates to be installed onto the end device to protect the integrity of the school data and equipment from viruses, malware, ransomware and alike.

Reporting faults

IT faults should be logged with the IT Support staff using the IT Helpdesk intranet page - http://gateway/staff/helpdesk.htm. This will allow IT staff to prioritise calls and work through them collaboratively. In the event that a network connection is unavailable staff may log the call in person or via telephone (x318), but must understand that a call will still be raised into the queuing system and that calls logged in person do not gain priority over existing calls.

Reporting E-Safety Concerns

Staff should report any e-safety or safeguarding concerns via the CPOMS system, which is accessible from the staff intranet dashboard or by visiting https://woodlandscc.cpoms.net/login.

Staff Summary of Important ICT AUP Rules

The SAUP will help to protect staff and the school by clearly stating what is acceptable and what is not. This page summarises some of the very explicit rules identified within this policy. Staff should however read, know and act in accordance with the policy as a whole.

- Access to the school IT Network resources must only be made by users authenticating their account and password, which must not be given to any other person. Passwords should be kept secure and should therefore not be written down or left unguarded at any time.

- School computer and Internet use (wired/wifi/4g) must be appropriate to teaching & learning, school work or professional development activities.

- Copyright and intellectual property rights must be respected.

- Users are responsible for e-mail they send and for contacts made.

- E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property.

- Attempts must not be made to send, access, save or display offensive messages or pictures on school equipment, within the perimeter of the school grounds or within work time if working from a remote site. In the unlikely event that any such material accidentally appears, an IT Support call should be logged immediately under category “inappropriate material”.

- The use of public chat rooms is prohibited, however the use of forums is acceptable if used for improving teaching and learning.

- Use of the ICT facilities for personal financial gain, gambling, political purposes or advertising is prohibited.

- The security of the school network and data must not be compromised:
  - Attempts should not be made to access unauthorised areas.
  - Users should not leave passwords unsecure i.e. record them in diaries, phones, pieces of paper, on the network etc.
  - Users should lock the use of all IT equipment, whether belonging to the school or a personal device; if leaving it unattended.
  - Sensitive data should be encrypted when saved onto personal devices, external hard drives or transmitted using digital systems.
  - Staff should use their own logins and should not allow others to use their login credentials as this can compromise the security of data or the school network.

- School equipment should be treated with respect. Any damage or theft to school equipment should be reported to IT Support via the IT Helpdesk on the staff intranet dashboard.

- Staff should only follow troubleshooting guidelines as published in the IT Induction Handbook and should not adjust or tamper with equipment or infrastructure without supervision from IT technical support staff.

- E-mail should be used in line with guidelines set out within this policy and checked regularly. Staff should endeavour to respond to email within 48 hours.

- BYOD. Any device brought in to school by staff must be looked after by that individual. The school does not hold responsibility for damage, theft, or corruption of any of these devices.

- Staff should consider the conduct of their social network activities as per the Social Networking section of this document. Breaches of social networking guidance could lead to disciplinary action.

- Staff have administrative permissions to install software onto computers allocated to them by the school. However, staff should be aware of the software packages that the school is able to provide them with from the Software Catalog (Appendix 3).

- To protect the security of the network some software is prohibited from being installed on any computer on Woodlands network. Staff should also ensure that they do not install any of the software listed on the Software Blacklist.

- Staff should report any e-safety or safeguarding concerns via the CPOMS system, which is accessible from the staff intranet dashboard or by visiting https://woodlandscc.cpoms.net/login.

- Where staff are planning to implement any new ICT system, then they should consult the schools' Data Protection Officer to establish whether a DPIA is required for GDPR compliance.

Student Acceptable Usage Policy (SAUP)

This section of the policy focuses its aim at students providing:

- acceptable usage information including restrictions placed upon users, equipment and the school reputation;
- guidelines on usage;
- guidance on E-Safety

It does not attempt to cover every possible scenario that may arise.

Introduction

The Internet, Intranet, e-mail, messaging systems and related technologies can be extremely valuable tools in an educational context, encouraging the development of communication skills, and transforming the learning process by opening up possibilities that, conventionally, would be impossible to achieve.   The school encourages the use of electronic mail as a medium for paper mail replacement and as a means of enhancing communications.

Creating a safe ICT learning environment includes three main elements at Woodlands:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- Access to E-Safety information for students, staff, parents and carers and other users;

All students should be familiar with the school E-Safety policy including:

- E-mail, messaging and digital communication (social networking) use;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as digital cameras and video cameras;
- Publication of student information/photographs and use of the Intranet and the school website;
- e-Bullying and Cyber-bullying procedures as per the school Behaviour for Learning policy;
- Their role in accessing E-Safety information;

Defining Unacceptable Use

The Internet, Intranet, email, messaging systems and related technologies must not be used for knowingly viewing, transmitting, retrieving, downloading or storing any communication that is:

- Discriminatory or harassing;
- Derogatory to any individual or group;
- Obscene or pornographic;
- Defamatory, threatening or seen as cyber bullying;
- Illegal or contrary to the schools' policies or business interests;
- Subject to Copyright such as music, software or films;
- Likely to cause network congestion or significantly hamper access for other users;
- Students may only play appropriate web based educational games during break or lunch times, unless directed by their class teacher; and must not install any games to the network.
- Students may only use school provided messaging systems at appropriate times if indicated by the teacher or during break or lunch time.

Students should also be conscious that uploading any of the above categories into the public domain may result have jeopardise the safety and security of students and/or staff and can have serious consequences.

Students must not:

- Use a mobile phone or similar technologies on the school site.
- Deface the schools' equipment;
- Vandalise school equipment, for example remove mouse balls/buttons, remove front plates to disk drives, damage keyboards;
- Load executable files or use those files to gain access to unauthorised areas of the network. For example gaining access to File Manager or Explorer.
- Seek/attempt illegal access to another user's area;
- Change the settings of stations, for example screen displays; desktop images;
- Use equipment to record or photograph other students or staff unless given permission to do so by a member of staff;
- Use USB drives or any removable storage devices unless regularly checked for viruses.

Failure to comply with any of the above items, will result in a minimum C3, 40 minute detention being issued.

Students use of school owned equipment at home

Students accessing the Internet from home whilst using a school owned computer or mobile device, or through school owned connections such as the Remote Desktop Connection (Home Link) must adhere to the policies set out in this document.

Family members or other 'non-School' users must not be allowed to access the school's computer system or use the school's computer facilities, without the formal agreement of the Head Teacher.

Parental Agreement for student use

All students must sign the Student/Parent Contract in order to gain access to the school network and subsequent internet connection. Any breaches of this policy may result in his/her removal from the network for a sustained period of time depending on the severity of the offence. In the event of damage to school equipment, network or files; the school reserves the right to charge parent/carers associated cost as a result of the offence.

Removal of Internet or computer access may ultimately prevent access to files held on the system, including student files or student examination coursework.

Woodlands monitors all aspects of ICT usage. All content must be polite and the school will monitor all usage including email and messages and may access or intercept this information.

Student Summary of Important ICT Rules

The Student Acceptable Use Policy will help to protect students and the school by clearly stating what is acceptable and what is not. This page summarises some of the very explicit rules identified within this policy. Students should however read, know and act in accordance with the Student Acceptable Use Policy as a whole. This will form part of the first lessons that students have in Year 7 on entry to the school.

- Use a mobile phone on the school site. Failure to comply with this rule will result in a C3 being issued along with a 40 minute detention.

- Access to the school IT Network resources must only be made by users authenticating their account and password, which must not be given to any other person. Passwords should be kept secure and should therefore not be written down or left unguarded at any time.

- School computer and Internet use (wired/wifi/4g) must be appropriate to teaching & learning, school work or professional development activities.

- Copyright and intellectual property rights must be respected.

- Users are responsible for e-mail they send and for contacts made.

- E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property.

- Attempts must not be made to send, access, save or display offensive messages or pictures on school equipment, within the perimeter of the school grounds or on online cloud storage applications such as Google Drive, social networks or any school VLE. In the unlikely event that any such material should accidentally appear on a computer that a student is logged onto they should notify their teacher immediately, who will log an IT Support call immediately under category “inappropriate material”.

- Use of the ICT facilities for personal financial gain, gambling, political purposes or advertising is prohibited.

- The security of the school network and data must not be compromised:
  - Attempts should not be made to access unauthorised areas.
  - Users should not leave passwords unsecure i.e. record them in diaries, phones, pieces of paper, on the network etc.
  - Users should lock the use of all IT equipment, whether belonging to the school or a personal device if leaving it unattended.
  - Sensitive data should be encrypted when saved onto personal devices or external hard drives.
  - Students should use their own logins and should not allow others to use their login credentials as this can compromise the security of data or the school network.

- School equipment should be treated with respect. Any damage or theft to school equipment should be reported to IT Support team, noting down specific error messages where applicable. Students may be liable for any cost incurred to the school as a result of an act of malicious damage.

- Students should not attempt to troubleshoot, adjust or tamper with equipment or infrastructure.

- BYOD - Any device brought in to school by a student, remains the responsibility of that student. The school cannot be held responsibility for damage, theft, or corruption of any of these devices.

- BYOD – Woodlands has a no mobile phone policy in place for all students.
  The BYOD Student Wi-Fi network may only be used outside of the school day (including detentions) for example when attending an evening club, weekend activity.

- Students are advised of the dangers of online communities through PD Days and should endeavour to remember these dangers at all times. If students require reminders or refresher sessions they should attempt to make an appointment with the E-Safety Co-ordinator.

- Students must not attempt to install any software onto school IT equipment. If additional software is required, students should ask their teacher to raise an IT Support call, and IT Support staff will audit the software and respond to the request accordingly.

Parental Guidelines and Agreement (PGA)

Parents/carers should read the introductory section and Student Acceptable Use Policy section above to ensure that they understand the rules and guidelines that are being set out by this policy. Parents may also wish to read the Staff Acceptable Use Policy (SAUP) section to understand the measures the school takes to ensure that acceptable use of ICT is adhered to by all.

On the following pages there is a letter from the Head Teacher outlining ICT acceptable use, along with the parent/student contract. This contract is given to every student in the school and must be completed prior to students using the schools computer systems and associated internet connection.

With the current speed of on-line change, some parents and carers have only a limited understanding of online risks and issues. Parents may underestimate how often their children come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. Some of the risks could be:

- unwanted contact
- grooming
- online bullying including sexting
- digital footprint

The school will therefore seek to provide information and awareness to both students and their parents through:

- This policy and its associated guidelines and recommendations
- Curriculum activities involving raising awareness around staying safe online
- Information included in letters, newsletters, web site, VLE
- Parents evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Building awareness around information that is held on relevant web sites and or publications

The school also recognises the following websites as giving valuable e-safety advice:

National Agencies, Charities and Support

- Child Exploitation and Online Protection centre - report concerns to CEOP via the "Click CEOP" button
- Virtual Global Taskforce - making the internet safer for children
- Think U Know - advice for parents, teachers and young people and teaching resources
- Internet Watch Foundation - report illegal content online
- Childnet International – guidance for parents, teachers, children and young people
- UK Safer Internet Centre - e-safety tips and resources
- NSPCC Online Safety – NSPCC Online Safety advice
- Action Fraud - report consumer and online fraud
- The Marie Collins Foundation - helping children who are abused online
- The Lucy Faithfull Foundation - Advice, self-help and educational programmes about online abuse
- The Samaritans - Supporting Schools - support for young people in schools including giving talks to schools and teaching resources
- Papyrus - prevention of young suicide
- Young Minds - improving the emotional well-being of children and young people.
- Childline - NSPCC Childline Service
- Professional Online Safety Helpline: www.saferinternet.org.uk, helpline@saferinternet.org.uk or 0844 381 4772
- Revenge Porn Helpline (NB if the person is under 18 please report to CEOP/Kent Police)

- Stop Online Abuse – Report online Sexism, homophobia, biphobia and transphobia
- Anti-Bullying Alliance

Woodlands

• Inspiring • Challenging • Achieving •

Head Teacher: Mr J Henderson BA (Hons) NPQH

Dear Parent/Carer

Responsible ICT Use

As part of your child's curriculum and the development of computing skills, Woodlands Community College provides supervised access to the Internet. We believe that the use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world.

The school takes positive steps to try and ensure that students do not have access to undesirable material. The school operates a dual-layer content filtering system that restricts access to inappropriate materials. This may not be the case at home and parents are therefore able to gain advice from the E-Safety section on our website (http://www.woodlands.southampton.sch.uk/safeguarding-e-safety/).

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The school will not be liable for any damages arising from your child's use of the Internet facilities.

I would also remind parents that the use of mobile phones by students is not permitted.

A full copy of the ICT Acceptable Usage & E-Safety Policy is available on the school website policies page (http://www.woodlands.southampton.sch.uk/parental-info/policies/).

Additionally the schools' student privacy notice is listed on our website. This notice includes details of third parties that the school may exchange student personal information with, using public interest as the legal basis for the processing of the information.

Yours sincerely

J Henderson

Mr J Henderson
Head Teacher

Minstead Avenue, Harefield,
Southampton SO18 5FW
Telephone: 023 8046 2322
023 8046 3303 (24*hr*)
023 8047 4866 (*Community Office*)
Fax: 023 8046 2342
Email: info@woodlands.southampton.sch.uk
Website: www.woodlands.southampton.sch.uk

Woodlands Community College

ICT Acceptable Use Policy

Student/Parent Consent

Please take time to discuss this document with your child and then complete, sign and return to the school.

Student Name:	Tutor:	House:	Year:

Student's Agreement

I have read and understood the Student Summary of Important ICT Rules. I will use the schools' digital systems, BYOD and Internet in a responsible way and follow these rules at all times. I understand that my parents/carers will be expected to pay for any damage I cause to equipment and / or a BYOD.

Student Signature:	Date:

Parent's Consent for access to technology

I have read and understood the Parental Guidelines and Agreement (PGaA) and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure students cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities. I understand that I will be charged if my son/daughter damages any equipment. The school will not be held responsible for any damage or theft of a BYOD.

Parent/Carer Signature:	Date:
Please print name:	

Parent's Consent for Web Publication of Work and Photographs

I agree that, if selected, my son/daughter's work (including their name) may be published on the school Web site or affiliated sites.

Parent/Carer Signature:	Date:

I agree that, if selected, my son/daughter's photograph may be published on the school Web site, other affiliated sites and any other school publications.

Parent/Carer Signature:	Date:

Key Contacts

Role	Named Contact	Email Address
Head Teacher	Mr J Henderson	head@woodlands.southampton.sch.uk
Whole School Leader of ICT/E-Safety Co-Ordinator	VACANT	
Line Manager of Whole School Leader of ICT/E-Safety Co-Ordinator	Mr C Main	colin.main@woodlands.southampton.sch.uk
Data Protection Officer	Mrs J Edwards	jenny.edwards@woodlands.southampton.sch.uk
Designated Safeguarding Lead	Miss N Iverson	nicola.iverson@woodlands.southampton.sch.uk
Designated Safeguarding Lead	Mrs D Lowth	diane.lowth@woodlands.southampton.sch.uk
Designated Safeguarding Lead	Mrs M Pearce	michelle.pearce@woodlands.southampton.sch.uk
Designated Safeguarding Lead	Mr S Crowe	simon.crowe@woodlands.southampton.sch.uk
Line Manager for IT Support	Mr N Obee	nick.obee@woodlands.southampton.sch.uk
Senior IT Technician	Mr S Gray	sam.gray@woodlands.southampton.sch.uk

Appendix 1 – Website and inappropriate materials categories

Woodlands operates two levels of website content filtering:

- Lightspeed hardware bottle rocket – this is a specialised onsite device, which updates live directly from Lightspeed Systems servers adding any new websites to a category outlined in the table below.
- Impero Education Pro – this is a network tool for IT Administrators and staff. The tool includes a further layer of content filtering categories which can be applied to groups or individual computers or users.

Parent Category	Sub-category with definitions	Blocked/Open
Abortion		Open
Sites with neutral or balanced presentation of the issue.	Pro-Choice -- Sites that provide information about or are sponsored by organisations that support legal abortion or that offer support or encouragement to those seeking the procedure.	Open
	Pro-Life -- Sites that provide information about or are sponsored by organisations that oppose legal abortion or that seek increased restriction of abortion	Open
Adult Material		
Parent category that contains the categories:	Adult Content -- Sites that display full or partial nudity in a sexual context, but not sexual activity; erotica; sexual paraphernalia; sex-oriented businesses as clubs, nightclubs, escort services; and sites supporting the online purchase of such goods and services.	Blocked
	Lingerie and Swimsuit -- Sites that offer images of models in suggestive but not lewd costume, with seminudity permitted. Includes classic 'cheese-cake,' calendar, and pinup art and photography. Includes also sites offering lingerie or swimwear for sale.	Blocked
	Nudity -- Sites that offer depictions of nude or seminude human forms, singly or in groups, not overtly sexual in intent or effect.	Blocked
	Sex -- Sites that depict or graphically describe sexual acts or activity, including exhibitionism; also sites offering direct links to such sites.	Blocked
	Sex Education -- Sites that offer information about sex and sexuality, with no pornographic intent.	Open
Advocacy Groups		

Sites that promote change or reform in public policy, public opinion, social practice, economic activities and relationships.	No sub-categories	Open
Bandwidth Categories		
Parent category that contains the categories:	Internet Radio and TV -- Sites whose primary purpose is to provide radio or TV programming on the internet.	Open
	Internet Telephony -- Sites that enable users to make telephone calls via the Internet or to obtain information or software for that purpose.	Blocked
	Peer-to-Peer File Sharing -- Sites that provide client software to enable peer-to-peer file sharing and transfer.	Blocked
	Personal Network Storage and Backup -- Sites that store personal files on Internet servers for backup or exchange.	Blocked
	Streaming Media -- Sites that primarily provide streaming media content, such as movie trailers.	Blocked
Business & Economy		Open
Sites sponsored by or devoted to business firms, business associations, industry groups, or business in general.	Financial Data and Services -- Sites that offer news and quotations on stocks, bonds, and other investment vehicles, investment advice, but not online trading. Includes banks, credit unions, credit cards, and insurance.	Open
Drugs		
Parent category that contains the categories:	Abused Drugs -- Sites that promote or provide information about the use of prohibited drugs, except marijuana, or the abuse or unsanctioned use of controlled or regulated drugs; also, paraphernalia associated with such use or abuse.	Blocked
	Marijuana -- Sites that provide information about or promote the cultivation, preparation, or use of marijuana.	Blocked
	Prescribed Medications -- Sites that provide information about approved drugs and their medical use.	Open
	Supplements and Unregulated Compounds -- Sites that provide information about or promote the sale or use of chemicals not regulated by the FDA (such as naturally occurring compounds).	Open
Education		Open

Parent category that contains the categories:	Cultural Institutions -- Sites sponsored by museums, galleries, theatres, libraries, and similar institutions; also, sites whose purpose is the display of artworks.	Open
	Educational Institutions -- Sites sponsored by schools and other educational facilities, by non-academic research institutions, or that relate to educational events and activities.	Open
	Educational Materials -- Sites that provide information about or that sell or provide curriculum materials or direct instruction; also, learned journals and similar publications.	Open
	Reference Materials -- Sites that offer reference-shelf content such as atlases, dictionaries, encyclopedias, formularies, white and yellow pages, and public statistical data.	Open
Entertainment		
Parent category that contains the categories:	Sites that provide information about or promote motion pictures, non-news radio and television, books, humour, and magazines.	Open
	MP3 and Audio Download Services -- Sites that support downloading of MP3 or other sound files or that serve as directories of such sites.	Blocked
Gambling		
Sites that provide information about or promote gambling or support online gambling, involving a risk of losing money.	No sub-categories	Blocked
Games		
Parent category that contains the categories:	Sites that provide information about or promote electronic games, video games, computer games, role-playing games, or online games. Includes sweepstakes and giveaways.	Blocked
	Educational Games - Sites that provide access to games with educational enrichment	Open
Government		Open
Sites sponsored by branches, bureaus, or agencies of any level of government, except for the armed forces.	Military -- Sites sponsored by branches or agencies of the armed services.	Open

	Political Organisations -- Sites sponsored by or providing information about political parties and interest groups focused on elections or legislation.	Open
Health		
Sites that provide information or advice on personal health or medical services, procedures, or devices, but not drugs. Includes self-help groups.	No sub-categories	Open
Illegal or Questionable		
Sites that provide instruction in or promote nonviolent crime or unethical or dishonest behaviour or the avoidance of prosecution.	No sub-categories	Blocked
Information Technology		
Parent category that contains the categories:	Sites sponsored by or providing information about computers, software, the Internet, and related business firms, including sites supporting the sale of hardware, software, peripherals, and services.	Open
	Computer Security -- Sites that provide information about or free downloadable tools for computer security.	Blocked
	Hacking -- Sites that provide information about or promote illegal or questionable access to or use of computer or communication equipment, software, or databases.	Blocked
	Proxy Avoidance -- Sites that provide information about how to bypass proxy server features or to gain access to URLs in any way that bypasses the proxy server.	Blocked
	Search Engines and Portals -- Sites that support searching the Web, news groups, or indices or directories thereof.	Open
	URL Translation Sites -- Sites that offer online translation of URLs. These sites access the URL to be translated in a way that bypasses the proxy server, potentially allowing unauthorised access.	Blocked
	Web Hosting -- Sites of organisations that provide hosting services, or top-level domain pages of Web communities.	Open
Internet Communication		

Parent category that contains the categories: Email, Web Chat	Web Chat -- Sites that host Web chat services or that support or provide information about chat via HTTP or IRC.	Blocked
	Organisational Email - Sites that host organisational email	Blocked
	General Email -- Sites that host Web-based email.	Open
	Text and media messaging - sites that enable users to send texts from their PCs	Blocked
Job Search		
Sites that offer information about or support the seeking of employment or employees.	No sub-categories	Open
Militancy and Extremist		
Sites that offer information about or promote or are sponsored by groups advocating anti-government beliefs or action.	No sub-categories	Blocked
Miscellaneous		
Parent category that contains the categories:	Content Delivery Networks -- Commercial hosts that deliver content to subscribing Web sites.	Blocked
	Dynamic Content -- URLs that are generated dynamically by a Web server.	Open
	File Download Servers -- Web servers whose primary function is to deliver files for download.	Blocked
	Image Servers -- Web servers whose primary function is to deliver images.	Open
	Images (Media) -- URLs ending with image filenames.	Open
	Network Errors -- URLs with hosts that do not resolve to IP addresses.	Open
	Private IP Addresses -- IP addresses defined in RFC 1918, 'Address Allocation for Private Intranets'	Open
	Uncategorised -- Sites not categorised in the EIM Database.	Blocked
News & Media		
Parent category that contains the categories:	Sites that offer current news and opinion, including those sponsored by newspapers, general-circulation magazines, or other media.	Open
	Alternative Journals -- Online equivalents to supermarket tabloids and other fringe publications.	Open

Productivity Categories		
Parent category that contains the categories:	Advertisements -- Sites that provide advertising graphics or other ad content files.	Blocked
	Freeware and Software Download -- Sites whose primary function is to provide freeware and software downloads.	Blocked
	Instant Messaging -- Sites that enable instant messaging.	Blocked
	Message Boards & Forums -- Sites for online personal and business clubs, discussion groups, message boards, and list servers; includes 'blogs' and 'mail magazines.'	Open
	Online Brokerage and Trading -- Sites that support active trading of securities and management of investments.	Blocked
	Pay-to-Surf -- Sites that pay users to view Web sites, advertisements, or email.	Blocked
Racism and Hate		
Sites that promote the identification of racial groups, the denigration or subjection of groups, or the superiority of any group.	No sub-categories	Blocked
Religion		
Parent category that contains the categories:	Non-Traditional Religions and Occult and Folklore -- Sites that provide information about or promote religions not specified in Traditional Religions or other unconventional, cultic, or folkloric beliefs and practices.	Open
	Traditional Religions -- Sites that provide information about or promote Bahai, Buddhism,Christian Science, Christianity, Hinduism, Islam, Judaism, Mormonism, Shinto, and Sikhism, as well as atheism.	Open
Security		
Sites that have been identified as causing a cyber-security risk to network or individuals	security.hacking – Sites that contain tools, how to descriptions or are used to perform computer hacking	Open to IT Staff for research
	security.malware – Combines the Security.virus, Security.spyware and Security.phishing categories on Lightspeed Rockets.	Open to IT Staff for research
	security.nettools – Sites that contain administrative tools that may be used to bypass network security or content filter. Examples include	Open to IT Staff

	VPN products, remote access products like logmein.com, teamviewer.com and forum sites or blogs with tutorials or products to bypass workstation security and reset admin passwords.	
	security.phishing – Scam sites that try to collect users identity information by posing as legitimate sites such as banks or government agencies and then recording information the user enters. We get a large number of these domains from sites that track and identify phishing attacks such as phishtank.org.	Open to IT Staff for research
	security.potentially unwanted_applications – Potentially unwanted applications that contain adware, install toolbars or have other unclear objectives.	Open to IT Staff for research
	security.spyware – Sites that install programs or cookies for the purpose of tracking the users keystrokes, search activities and other information for use in targeting advertising to the user as well as selling the information to third parties	Open to IT Staff for research
	security.translators – Language translation sites that allow full URL (webpage) translation and DO NOT honour filter restrictions	Blocked
	security.virus – Sites that contain viruses, malware, trojans, and backdoors. Also sites that are being used by malware as command and control servers or to distribute virus payloads. These sites are identified through our malware research as well as by our categorization engine scanning every executable file that we find on a site to identify malware. We also identify sites through customer reports as well as security alerts when we are manually reviewing a site. Sites in this category are frequently checked and re-categorized once the threat is removed.	Blocked
	security.warez – Sites promoting illegal access and sharing of software and other copyrighted material	Blocked
Shopping		
Parent category that contains the categories:	Sites that support the online purchase of consumer goods and services except: sexual materials, lingerie, swimwear, investments,	Open

	medications, educational materials, computer software or hardware, alcohol, tobacco, travel, vehicles and parts, weapons.	
	Internet Auctions -- Sites that support the offering and purchasing of goods between individuals.	Blocked
	Real Estate -- Sites that provide information about renting, buying, selling, or financing residential real estate.	Open
Social Organisations		
Parent category that contains the categories:	Professional and Worker Organisations -- Sites sponsored by or that support or offer information about organisations devoted to professional advancement or workers' interests.	Open
	Service and Philanthropic Organisations -- Sites sponsored by or that support or offer information about organisations devoted to doing good as their primary activity.	Open
	Social and Affiliation Organisations -- Sites sponsored by or that support or offer information about organisations devoted chiefly to socialising or common interests other than philanthropy or professional advancement.	Open
Society & Lifestyle		
Parent category that contains the categories:	Sites that provide information about matters of daily life, excluding entertainment, health, hobbies, jobs, sex, and sports.	Open
	Alcohol and Tobacco -- Sites that provide information about, promote, or support the sale of alcoholic beverages or tobacco products or associated paraphernalia.	Blocked
	Gay or Lesbian or Bisexual Interest -- Sites that provide information about or cater to gay, lesbian, or bisexual lifestyles, including those that support online shopping, but excluding those that are sexually or issue-oriented.	Open
	Hobbies -- Sites that provide information about or promote private and largely sedentary pastimes, but not electronic, video, or online games.	Open
	Personals and Dating -- Sites that assist users in establishing interpersonal relationships, excluding those intended to arrange for	Blocked

	sexual encounters and excluding those of exclusively gay or lesbian or bisexual interest.	
	Restaurants and Dining -- Sites that list, review, advertise, or promote food, dining, or catering services.	Open
	Social Networking and Personal Sites - Sites chiefly devoted to personal expression by individuals (as in diaries or personal blogs) or small groups, often but not necessarily involving multiple links to similar sites.	Some now open to staff to allow for school reputation growth on social media
Special Events		
Sites devoted to a current event that requires separate categorisation.	No sub-categories	Open
Sports		Open
Parent category that contains the categories:	Sites that provide information about or promote sports, active games, and recreation.	Open
	Sport Hunting and Gun Clubs -- Sites that provide information about or directories of gun clubs and similar groups, including war-game and paintball facilities.	Blocked
Tasteless		
Sites with content that is gratuitously offensive or shocking, but not violent or frightening. Includes sites devoted in part or whole to scatology and similar topics or to improper language, humour, or behaviour.	No sub-categories	Blocked
Travel		
Sites that provide information about or promote travel-related services and destinations.	No sub-categories	Open
User-Defined		
User-defined category	No sub-categories	None
Vehicles		

Sites that provide information about or promote vehicles, including those that support online purchase of vehicles or parts.	No sub-categories	Open
Violence		
Sites that feature or promote violence or bodily harm, including self-inflicted harm; or that gratuitously display images of death, gore, or injury; or that feature images or descriptions that are grotesque or frightening and of no redeeming value.	Violence.extremism – Sites that encourage or promote violence to further a set of beliefs or agenda, or attempt to convert others to view that violence is appropriate to further a set of beliefs or an agenda. CANNOT BE UNBLOCKED. This category contains data provided through our association with the UK Home Office linked to radicalisation.	Blocked
	Violence.hate – Sites that promote hate against different group	
Weapons		
Sites that provide information about, promote, or support the sale of weapons and related items.	No sub categories	Blocked

Appendix 2 – Legal Framework

There are numerous laws that apply to the use of information and its processing. This page sets out what the laws and regulations are and what you must do to ensure that you comply with them.

The Data Protection Act 1998 (Now GDPR 2018)

The Data Protection Act of 1998 has now been replaced by the GDPR as of May 25th 2018. The GDPR sets out seven key principles, which are broadly similar to the eight principles that were previously identified in The Data Protection Act 1998 and can be seen in the table below.

Data Protection Act 1998	The GDPR 2018
1st principle - Fairness: personal information must be processed fairly and lawfully. A key point is that the individual must have given his or her consent to the information being processed.	Principle (a) – lawfulness, fairness and transparency. *Article 5(1) requires that personal data shall be* (a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
2nd principle - Purpose: personal information must only be used for the purposes for which it is obtained and no other	Principle (b) – purpose limitation *Article 5(1) requires that personal data shall be:* (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
3rd principle - Relevance: personal information must be adequate (enough to process it), relevant and not excessive (not asking for more than is needed)	Principle (c) – data minimisation *Article 5(1) requires that personal data shall be:* (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
4th principle - Accuracy: personal information must be accurate and up to date	Principle (d) – accuracy *Article 5(1) requires that personal data shall be:* (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
5th principle - Preservation: personal information must only be held for as long as is necessary to complete the purpose for which it was obtained	Principle (e) – storage limitation *Article 5(1) requires that personal data shall be:* (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures

	required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
6th principle - Rights of the individual: personal information must only be used in accordance with the rights of the individual	Principle (f) – integrity and confidentiality *Article 5(1) requires that personal data shall be:* (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."
7th principle - Security: we must take appropriate measures to: • Keep the personal information secure • Prevent unauthorised or unlawful use or access to it • Prevent damage or accidental loss	Principle (g) – Accountability *Article 5(2) adds that:* "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."
8th principle - Transfer of personal data: we cannot transfer personal data to a country or territory outside of the European Economic Area (EEA) unless that country is able to demonstrate that an adequate level of protection exists for the processing of the data.	

However there are a few key changes. Most obviously:

- Principle 6 (Rights of the individual) has been removed.
  This is now dealt with separately in Chapter III of the GDPR;
- Principle 8 (Transfer of personal data) has been removed.
  This is now dealt with separately in Chapter V of the GDPR;
- There is a new accountability principle (g).
  This specifically requires organisations to take responsibility for complying with the principles, and to have appropriate processes and records in place to demonstrate compliance.

In reference to the removal of Principle 6 (Rights of the individual), the GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

In reference to the removal of Principle 8 (Transfer of personal data), the GDPR provides the following rights for individuals:

- Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

ISO/IEC 27001

The information security policy embraces all of the principles of ISO/IEC 27001 and the Information Commissioner has indicated that organisations complying with ISO/IEC 27001 will have gone a long way towards satisfying the information security requirements of the Data Protection Act 1998.

The Computer Misuse Act 1990

This Act permits the prosecution of anyone who accesses, or attempts to access a computer system or information that they are not authorised to access. This means that if you have only been given certain access rights to information, you mustn't try to view information to which you haven't been given rights.

The Copyright, Designs and Patents Act 1988

Computer software is covered by this Act. This means that you must only use properly licensed software and only as far as the licence allows. You must not take illegal copies of the software, or use unlicensed software on Council computer systems. If you expose the Council to the risk of prosecution under this Act, you could be subject to disciplinary action.

Electronic Communications Act 2000

This Act gives legal status to the use of digital signatures and their associated certificates. If you are transmitting personal data, you must make use of the cryptographic facilities available in the Council.

Regulation of Investigatory Powers Act 2000

This Act governs the circumstances in which an organisation is allowed to intercept communications to and from its networks, including that of employees. You must therefore be aware that you have no right to expect privacy in relation to any information that you store or transmit across Council systems. However, the Council will only monitor your activities under the framework of the above act.

Freedom of Information Act 2000

This Act gives anyone anywhere in the world the right to ask for information from us, to which we are obliged to respond. However, you must not give out information without first checking that you are allowed to disclose it, and that the person who is asking for it is authorised to see it. For example, you are not allowed to give personal information to anyone other than to the person to whom it applies, or commercially sensitive information.

Appendix 3 – Software Catalog

Please be aware that Woodlands can provide access to the software below. However, some of the packages may be limited in terms of which devices they can be installed on or indeed how many licences the school has for them. All requests for additional software should be logged as an IT Support Call.

If staff are at all unsure about the safety of a particular piece of software that they would like to install they should consult the IT Support Team.

Woodlands Licenced Software	Additional Open Source Software	Blacklisted Software (not to be used)
• Microsoft Windows XP • Microsoft Server 2008 • Microsoft Windows 7 • Microsoft Windows 10 • Microsoft Office 2003 • Microsoft Office 2010 • Microsoft Office 2013 • Microsoft Office 2016 • Capita Sims.Net • Sims InTouch • Sims Parent • Impero Console • LiveDrive • Promethean Activ Studio • Promethean Activ Inspire • Starboard 7.0 • Genie Backup Manager • Eclipse and MLS Connect • Comic Life • Lexia Reading • LOGIT Lab 4 • Lucid LASS • Lucid Memory Booster • Lucid Exact • Techsoft 2D Design • Techsoft 2D Design V2 • Exam Wizard PE • PCB Wizard • Livewire • Control Studio • Papercut • Serif Media Suite • Visit-ED • Tucasi Schools Cash Office • Show My Homework • Lexia • CPOMS • SISRA Online • SISRA Analytics • Eclipse	• Google Chrome • Google Apps Sync • Google Drive • Google Classroom • Dropbox • Free Studio • Safari • Quicktime • ITunes • VLC Player • Picasa • Movie Maker • 7-Zip • Daemon Tools Lite • Astroburn • Google Earth • ICloud • Screen-Cast-O-Matic • Wink • Hat Randomiser • Microsoft Security Essentials • Shrewsoft VPN Client • Adobe Premiere Pro 2.0 • Adobe Audition 3.0 • Adobe Photoshop CS2 • Fortinet VPN SSL Client • Teamviewer	• Napster • Morpheus • UTorrent • Any Peer-to-peer file sharing • Any other virus protection

Appendix 4 - Email and Messaging – Good Practice Guide

	Good Practice
Read Receipt	When it is important to know that a recipient has opened a message, it is recommended that the sender invoke the ‘read receipt’ option.
Attachment Formats	When attaching a file it will have a specific format. Be aware of the possibility that a recipient may not have the software necessary to read the attachment. Format incompatibility can occur even between successive versions of the same software, e.g. different version of Microsoft Word.
Email Address Groups	If messages are regularly sent to the same group of people, the addressing process can be speeded up by the creation of a personal group in the personal address book.
Message header, or subject	Convey as much information as possible within the size limitation. This will help those who get a lot of Emails to decide which are most important, or to spot one they are waiting for.
Subject	Avoid sending messages dealing with more than one subject. These are difficult to give a meaningful subject heading to, difficult for the recipient to forward on to others for action, and difficult to archive.
Recipients	Beware of sending messages to too many recipients at once. When sending messages for more than one-person’s use be sure to indicate people for whom there is some expectation of action or who have central interest. cc to indicate those who have peripheral interest and who are not expected to take action or respond unless they wish to do so.
Replying	When replying to a message sent to more than one person, do not routinely reply to all recipients of the original message. Consider who needs to read your reply, e.g. if the sender is organising a meeting and asking you for availability dates, you need only reply to the sender.
Absent	If you have your own Email address, it is possible, for users of MS Exchange or have local enhancements to MS-mail, to set the ‘out of office’ message when you are going to be away for some time, e.g. on annual leave. You won’t lose your messages, they will await your return, but the sender will know that you’re not there and can take alternative action if necessary.
Evidential Record	Never forget that electronic conversations can produce an evidential record which is absent in a telephone conversation. Comments made by an employee during the course of an exchange of Emails could be used in support, or in defence, of the Academy’s legal position in the event of a dispute.
Legal records	Computer generated information can now be used in evidence in the courts. Conversations conducted over the Email can result in legally binding contracts being put into place.
Distribution Lists	Keep personal distribution lists up-to-date and ensure you remove individuals from lists that no longer apply to them.
Email threads	Include the previous message when making a reply. This is called a thread. Threads are a series of responses to an original message. It is best that a response to a message is continued by using reply accessed on the quick menu bar, rather than start an entirely new message for a response. Keep the thread information together. It is easier for the participants to follow the chain of information already

	exchanged. If the message gets too long the previous parts can be edited while still leaving the essence of the message.
Context	Email in the right context, care should be taken to use Email where appropriate. There may be occasions when a telephone call would be more appropriate especially on delicate matters. Beware of the use of excessive use of capitals. It can be interpreted as SHOUTING so consider how the style of your email may be interpreted by its recipient.
Forwarding Emails	Consideration should be given when forwarding Emails that it may contain information that you should consult with the originator before passing to someone else.

Appendix 5 – Social Networking Letter – May 2016

Woodlands

• Respect • Responsibility • Resilience •

Head Teacher: Mr J Henderson BA (Hons) NPQH

First written - 16th May 2016

Dear Parents and Carers,

We continue to be extremely grateful for the partnership we have with you on all matters of your child's progress and wellbeing; it is in that spirit that we would like to make a specific plea to you about the use some children are choosing to make of social media. There have been a number of incidents this year with students using social media inappropriately. Often this has led to friendship issues and at times has led to students putting themselves and others in a vulnerable position. In the worst scenarios this has led to police involvement.

Students are particularly using Facebook, Instagram and Snap Chat in a way which sometimes leads to other students feeling attacked and victimised. The use of these is often unpleasant and unkind and, even if it is not directed at anyone specifically, uses an inappropriate level of abusive and sexually explicit language. This is mostly taking place outside of school in the evenings, and often takes place within a group-chat forum. However, it often then spills into school the next day and detracts from learning. Whilst we, as a school, cannot have control over what a student chooses to post on these forums, we do have a duty to deal with the fallout and the consequences when these come into school. Often it can have very upsetting effects on individuals and groups of students. Not only are these posts seen by lots of other people, who then pass further comment, they are also then a matter of public record. The consequences are potentially distressing and serious both for those who have written the unkind or unpleasant things, and for those at whom these comments are directed.

In the last week we have also been alerted to a new form of social media called Periscope. This allows the user to live stream from anywhere and to engage in conversations online during the live stream. It has come to my attention that a student has been live streaming from school. This is absolutely unacceptable. We take the safeguarding of our young people extremely seriously and using this form of social media within the school confines potentially puts our young people at risk. I have spoken to all students about this and made it clear that if anyone is caught doing this, the most severe sanctions will be placed upon those found doing so.

I would ask that you have a conversation with your child regarding their use of social media. Please could you ensure that they understand that the school will take a very serious view, via our behaviour and anti-bullying policies, towards any student choosing to behave with a lack of regard for the feelings of others in what they post. Additionally, the use of sexualised and aggressive language either directly towards any studentl online, or within a conversation that is then reported to us, will also warrant serious consequences.

Lastly, could you please also ensure that should your child be subjected to any issues online in the ways discussed in this letter, that you print copies or take screenshots and copy the comments and posts. These should then be reported to the police and to us in school. This allows us to follow up on any incidents that occur.

We truly believe that a robust stance on this is essential in a school that values the safety and wellbeing of its children and staff. If you have any questions about the contents of this letter, please do not hesitate to contact us at school.

With our thanks for your continued support,

Yours sincerely,

JHenderson

Mr J Henderson
Head Teacher
head@woodlands.southampton.sch.uk

Appendix 6 – Changes to the Behaviour for Learning Policy from 2016-17 in relation to mobile phones

The Behaviour for Learning Policy remains essentially the same and can be found on our website. However, as communicated in our weekly newsletter, from September 2016 we will be a no mobile phone school. This decision has not been taken lightly but in response to parental requests and a growing need to protect our young people from the dangers of social media, students should not have a visible phone in school. This means anywhere on the school premises during school time. Should they be seen with a phone on show at any time in the school day, they will be issued with a 40 minute detention.

For parents that would like their children to have a phone with them for travelling home, there is no reason why your son or daughter cannot have a phone in their bag during the school day which they can switch back on after school has ended. We would request though that these are not visible in the school day.

Should you need to get a message to your child please contact the school number and a message will be delivered. Should your child need to contact you urgently they should speak to the Assistant Year Leader who will ensure communication is facilitated.