respect resilience responsibility

ICT Acceptable Use & Online E-Safety Policy

Date: April 2026

Review Date: April 2027

Rationale

This policy is set out in three sections in order to cover the main areas where information technology is prevalent in school. These are…

1. The ICT curriculum
2. The delivery of online safety guidance through the PSHE curriculum and the values programme
3. Guidance for staff and students and parents

It outlines the range of the schools' technology systems and what is deemed as acceptable usage of these systems. These technologies encourage the development of communication skills and transform the learning process for all. This policy sets out the expectations of staff, students and other users (working for or on behalf of Woodlands Community College).

This policy is designed to express Woodlands' philosophy with regard to the Internet, Intranet and electronic communication and 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.

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 online 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 – 7 & 10	Maths Watch VLE
Apple Macs	Mac OS Operating System	Lexia Reading
Radio Studio	Windows Server 2008, 2012, 2016, 2019	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
Chromebooks	Logit Lab	Sims Parent App
	Lucid LASS	Sims Parents Evening System
New All in One PCs	Lucid Memory Booster	Parent Pay
Servers	Lucid Exact	Show My Homework
	Techsoft 2d Design & 2D Design V2	Impero
	Exam Wizard PE	Inventry
	PCD Wizard	ClassCharts
	Livewire	Parent Pay
	Python	Libresoft
	Pygame	SparX
	Control Studio	Educake
	Serif Media Suite – photo editor, web designer, video studio	Pinpoint Maths
	Microsoft Security Essentials	White Rose Maths
	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 latest DfE guidance on Keeping Children Safe in Education.

Section 1 – ICT Curriculum

All students have discrete ICT lessons in KS3.

Curriculum Vision.
'To give students a broad range of high quality skills and knowledge to thrive and make the most of opportunities in the digital world'
The curriculum is designed to establish a digital literacy students need for the 21st Century, foster a passion in computing and digital technology, and build the foundations of skills and knowledge required for further study as well as use of digital applications in future life.

The overall aims of the course are for students to be able to:

- Independently and confidently use a range of software (including spreadsheets, databases, graphic manipulation, drawing software and website building software) to be able to produce high quality intended outcomes.
- Confidently and independently be able to program using text based languages understanding and applying techniques of sequencing, variables, selection, iteration, functions and arrays to produce programs which work as intended.
- To recognise the computer –its operations, its functions, communication and storage – all work using binary; from the use of logic gates to control its FDE cycle, taking inputs and producing outputs, and storing information all result from binary.
- To understand all data is stored and operated as binary – bit patterns for text, images, sound and video
- To understand how information is transferred from one device to another, the protocols followed, the network structure and equipment needed.

Key Year 7 learning objectives:

- To understand how to log on to the school network, create files, use word and PowerPoint, save work and access the internet
- To understand the potential dangers of using the internet, how to avoid and report these dangers
- To understand and be able to use spreadsheets to record, store and process data
- To understand how to use a spreadsheet to perform functions on data.
- To understand how to use a spreadsheet to present data graphically.
- To understand what an algorithm is, how to represent algorithms visually and design solutions to everyday problems using an algorithm
- To understand what are and the importance of sequence, inputs and outputs, variables, selection and iteration in programming (using visual language)
- To be able to produce programs in a block based language apply sequence, inputs and outputs, variables, selection and iteration
- To recognise and describe the function of the key hardware, software, and peripherals of a PC
- To understand a computer stores information as binary and can convert binary to denary
- To understand how a computer uses the fetch decode execute to operate, and the links between memory and the CPU through the cycle
- To explain the purpose and stages of BIOS and the roles of an operating system in a computer.

Key Year 8 Learning objectives:

- To understand what are and the importance of sequence, inputs and outputs, variables, selection and iteration in programming.
- To be able to create programs using text-based programming language applying understanding of the principles of using variables, sequence, selection and libraries.
- To be able to use programming concepts to
- To understand what a network is, the benefits of using networks, and the difference in size between networks (LAN and WAN)
- To understand the hardware, topologies and types of different networks and how data is sent through the network to the correct device.
- To understand the threats to a computer network and how the network can reduce the threats by firewalls and encryption.
- To understand the importance of encryption and how information can be encrypted using a range of techniques.
- To be able to explain how vectors and bitmaps make images
- To be able to manipulate assets and present these as a digital graphic
- To understand what a database is and how a database is used to store, find and feedback
- To be able to create a databases and use queries and reports to interrogate the data stored

Key Year 9 learning objectives:

- To be able to apply principles of sequence, selection, iterations and variables when programming
- To be able to create programs using text-based programming language applying understanding of the principles of using iteration, if, else, and elif statements, random, and arrays.
- To understand how computers' convert and store text, images and sound as binary bit patterns
- To understand how digital devices' use binary (and Boolean logic) to operate gates which controls the function of the computer from storing information and manipulating data (adding)
- To understand how to add binary digits and convert from denary, to binary and hexadecimal.
- To be able to explain how vectors and bitmaps make images, the difference of
- To be able to manipulate assets effectively and present these as a digital graphic
- To be able to use a range of software effectively to acquire, repurpose and use different assets, considering composition and layout, to produce high quality digital graphics to meet the needs of a brief and target audience.

Section 2 – Delivery of online safety guidance through the PSHE Curriculum and the values programme

Online safety is a fundamental part of the PSHE and tutor time values programme of Respect, Responsibility and Resilience and is delivered to every year group in a variety of ways.

Year 7 – Respect

- the signs and effects of all types of bullying, including online
- how to respond to bullying of any kind, including online
- how to report and block online

Year 8 – Respect

- about the risks of 'sexting' and how to manage requests or pressure to send an image

Year 9 – Respect

- how the portrayal of relationships in the media and pornography might affect expectations
- how to assess and manage risks of sending, sharing or passing on sexual images
- how to access support services

Year 10 – Respect

- about the opportunities and risks of forming and conducting relationships online
- how to manage the impact of the media and pornography on sexual attitudes, expectations and behaviours
- about how social media may distort, misrepresent or target information in order to influence beliefs and opinions
- how to manage conflicting views and misleading information
- how to safely challenge discrimination, including online

Year 11 – Respect

- how to handle unwanted attention, including online
- how to challenge harassment and stalking, including online

Year 8 – Responsibility

- about online communication
- how to use social networking sites safely
- how to recognise online grooming in different forms, e.g. in relation to sexual or financial exploitation, extremism and radicalisation
- how to respond and seek support in cases of online grooming
- how to recognise biased or misleading information online
- how to critically assess different media sources
- how to distinguish between content which is publicly and privately shared
- about age restrictions when accessing different forms of media and how to make responsible decisions
- how to protect financial security online

Year 9 – Responsibility

- how to manage their 'personal brand' online
- how to identify and access support for concerns relating to life online

Year 10 - Responsibility

- How to be safe online concerning location settings, sharing of information with strangers etc…
- What to do if you feel pressured online
- Where and how to get support with online issues
- Catfishing
- Social media presence and links to employability

Year 7 – Resilience

- how to keep safe online

Year 8 – Resilience

- how to develop digital resilience

Year 9 - Resilience

- How to stay safe online by managing settings and protecting passwords
- Why do you need to be careful online, making positive choices
- Thinking carefully before commenting or posting online
- The laws and age limits for social media and gaming platforms and why they exist

Year 11 - Resilience

- about positive and safe ways to create content online and the opportunities this offers
- how to balance time online
- what is a money mule and how to avoid online scams
- online gambling and where to get help

Cyber Ambassadors Project

In addition to the PSHE and tutor time programme the school has signed up to run the Cyber Ambassadors project working with the Police and Crime Commissioners Office. Through the project a selection of staff and students will be trained in cyber safety by the Police Crime Commissioner's Office, share their knowledge and support their peers with cyber safety issues and work on school projects to raise awareness and create support for students in this area. This project has come about because of Ofsted's review of sexual abuse, where pupils said adults do not know the reality of their lives/ the extent of the problems within school and did not want to talk to adults about sexual harassment. This is why a peer-to-peer approach is successful, as pupils can relate to their peers and feel more comfortable speaking to them.

Section 3 – Guidance for staff and students and parents

Staff Training

The school delivers annual safeguarding training session to staff each September, which includes online 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.

- 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 concerning online safety on the Key Contacts Page.

- Every member of staff will 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
  - the process of radicalisation and how this might be identified early on through the use of online monitoring
  - how the school can provide support to ensure that our students are resilient and able to resist involvement in radical or extreme activities.

- Every member of staff will complete an annual certificate in online safety for schools in order to be able to identify risks young people face online, minimise the impact of online risk factors and support and guide young people to behave responsibly and safely online.

Attendance to the delivery of these training sessions are recorded and stored centrally

Students Online 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. See specifics above.

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 online safety page on the school website https://woodlands.southampton.sch.uk/wp-content/uploads/Online-safety-LFF-ELEC-Resource-Pack-for-Parents_MAY21-1.pdf that includes a live feed of online 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 Online 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 might 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 is provided with a school email account, 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 an 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
- Staff should also be extra vigilant when opening any email which requests any confidential information, or for them to click any links. Some attackers use a method of spoofing their identity in order to obtain such information or to encourage staff to click a link which may encrypt their system and/or compromise the security of the schools' data.
- When sending email, staff should consider carefully who needs to receive email, and make use of the appropriate distribution lists
- Staff should avoid sending emails out of working hours, including after 5:30pm in the evening.

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
- Send any confidential or personal data that may breach data protection rules

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 in an appropriate and professional manner.

Email signature blocks are set up 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 inappropriate language used throughout.

Woodlands Community College encourages a work life balance. Therefore, staff are encouraged not to send emails after 5.30pm, during school holidays or weekends.

Photographs and Video Images

Photographs or video images must not be taken in school unless they are for professional purposes. These should not be stored on personal devices or in personal cloud storage areas. Any photographs taken must be with the full consent of all parties contained within them.

Photographs or videos of students must not be used for any activity unless parental permission has been granted. The central list of photographic permissions can be accessed on the Intranet. Any photograph or video used for school purposes must have the consent of all parties.

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, if 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 that the forwarder could amend messages forwarded from another individual. 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
- Not 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

Online 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 online safety in the curriculum has been designated to the lead teacher for Digital Learning and the lead teacher of PSHE and is monitored by the relevant line managers to those staff.

The school also has an online safety working party whose role it is to meet once each half term to work on developing and reviewing the school's processes and systems in this area. This group is made up of a member of the senior leadership team, a school governor, the infrastructure manager, the curriculum leaders for Computing and PSHE and the staff lead for the cyber ambassadors project.

Referrals regarding online safety concerns should be logged by staff using the CPOMS system 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' online safety Co-ordinator ensures they keep up to date with 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's online safety co-ordinator ensures that the School Senior Leadership Team and 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 online safety issues and strategies. Where appropriate, the school will ensure Governors are aware of our local and national guidance on online safety and are updated annually on policy developments.

All staff are responsible for promoting and supporting safe behaviours in their classrooms and following online 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 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.
- cyber-bullying procedures as per the Behaviour for Learning Policy
- Their role in providing/accessing online safety information

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

Reporting student online 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 online 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 online safety co-ordinator

In cases where a student is found to have participated in a seriously breach of this policy, the online 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 online 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 online safety co-ordinator will track online safety incidents logged via CPOMS, and action them according to the schools' safeguarding policy. Where applicable the online 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

Guidance to staff on the appropriate use of Social Media is contained in our separate Social Media Policy. This document must be used alongside the ICT Acceptable Use Policy by all staff.

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. In line 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 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, by staff emailing to the IT Helpdesk - IT Support Desk. 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 (x1114), 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 Online safety Concerns

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

Student Acceptable Usage Policy (PAUP)

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 Online 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 Online safety information for students, staff, parents and carers and other users;

All students should be familiar with the school online 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 Online 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, 30 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.

Parental Guidelines and Agreement (PGA)

Parents/carers should read the introductory section and Student Acceptable Use Policy (PAUP) 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 school's 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 online 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 - online 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 about online abuse
- The Samaritans - Supporting Schools - support for young people in schools
- 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

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 Online safety section on our website (https://woodlands.southampton.sch.uk/wp-content/uploads/Online-safety-LFF-ELEC-Resource-Pack-for-Parents_MAY21-1.pdf).

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 & Online safety Policy is available on the school website policies page (https://woodlands.southampton.sch.uk/key-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



Mr J Henderson
Head Teacher

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
SLT responsible for overseeing online safety	Miss N Iverson	Nicola.Iverson@woodlands.southampton.sch.uk
Whole School Leader of Digital learning/online safety Co-Ordinator	Mr K Wooton	Kevin.wooton@woodlands.southampton.sch.uk
Lead teacher of PSHE	Mrs S Lambeth	sarah.lambeth@woodlands.southampton.sch.uk
Network Manager	Mr V Bitto	Viktor.Bitto@woodlands.southampton.sch.uk
Designated Safeguarding Lead	Miss N Iverson	Nicola.Iverson@woodlands.southampton.sch.uk
Senior IT Technician	Mr K Duffield	kieron.duffield@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 semi-nudity 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 semi-nude 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 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.	Open to IT Staff
	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, medications, educational materials, computer software or hardware, alcohol, tobacco, travel, vehicles and parts, weapons.	Open
	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 sexual encounters and excluding those of exclusively gay or lesbian or bisexual interest.	Blocked
	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 must not try to view information to which you have not 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 Server 2008, 2012, 2016, 2019 • Microsoft Windows 7, 10 • Microsoft Office 2003, 2010, 2013, 2016, 2019 • Capita Sims.Net • Sims InTouch • Sims Parent • Sims Parents Evening (SchoolCloud) • ShowMyHomework (Satchel1) • GDPRiS • 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 • Lexia • CPOMS • SISRA Online • SISRA Analytics • Eclipse (Reading Cloud) • Read Write Gold • ClassCharts	• 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 • Zoom • Loom	• Napster • Morpheus • UTorrent • Any Peer-to-peer file sharing • Any other virus protection

Appendix 4 - Email and Messaging – Good Practice Guide

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 School'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.