IT Policies

(Reviewer: Dan Higgins, August 2023)

1. IT Acceptable Usage Policy (Staff/Pupils)

Introduction

The College pays due regard to the Revised Prevent Duty Guidance: for England and Wales (April 2021) and, as such, will monitor on a daily basis, the use of internet by both staff and students.

All use of the computing and network facilities in Hurstpierpoint College, is subject to certain rules. These rules concern what is considered to be unacceptable behaviour and misuse, as well as what may infringe license terms or may be otherwise illegal. Your use of the College IT facilities and networks is restricted to authorized, bona fide, educational purposes only, such as those, which are consequent upon the teaching, study, research, administration or related activity occasioned by the employment or course of study with the College.

Misuse of computing and network facilities and unacceptable behaviour include (but are not limited to) the following:

- Attempting to gain unauthorized access to a resource or device.
- Using someone else's username and password.
- Disregarding the privacy of other people's files
- Giving your password to someone else, or being otherwise careless with it
- Generating messages, which appear to originate from someone else, or otherwise attempting to impersonate someone else
- Sending messages which are abusive or a nuisance or in any way potentially offensive or distressing
- Displaying offensive material
- Posting material onto a social media site that could be considered as disrespectful to individuals, or is obscene, sexually explicit, inappropriate, inflammatory or defamatory towards the College or any part of it.
- Trying to interfere with someone else's use of the facilities
- Disregard for "computer etiquette"
- Sending chain email
- Being wasteful of resources
- Software piracy (including infringement of software licenses or copyright provisions)
- Using the facilities for commercial gain without written authorization form College management
- Physically damaging or otherwise interfering with facilities
- Creating unnecessary network traffic
- Use or attempted use of any form of network analysis tools
- Attempting to modify or in any way alter software

Network Rules

Users of computers and mobile devices attached to the College network must not attempt to gain unauthorized access to or interfere with the operation of any other computer system, either within or outside the College. The College may bar access to any computer, mobile device or sub-network that appears to be used for such activities.

All email sent via the College network must correctly identify both the sender of the mail and the host or unit with which the sender is associated.

Network users must take all reasonable steps to ensure that they do not cause an excessive amount of network traffic on the College's internal networks or its external network links. The College may bar access at any time to computers or other device, which appear to cause unreasonable consumption of network resources. The College network or its external links may not, in general, be used to supply access to anything other than local services to any person who is not a member or employee of the College.

E-mail and Internet use

The College provides computing equipment and access to networks for the furtherance of the academic work of staff and students. It is a misuse of those facilities, and may in certain cases be illegal, for a user to receive, transmit, display or store offensive or pornographic material using

College equipment. Remember that sending email from your College is similar to sending a letter on a Hurstpierpoint College letterhead, so don't say anything that might discredit or bring embarrassment to the College.

E-Mail

- Don't pretend you are someone else when sending mail
- Don't send frivolous, abusive or defamatory messages. Apart from being discourteous or offensive, they may also break the law.
- Be tolerant of others mistakes. Some people may not be good typists, or they may accidentally delete your message and ask you to resend it.
- Remember that the various laws of the land relating to written communication apply equally to email messages, including the laws relating to defamation, copyright, fraudulent misrepresentation, freedom of information, and wrongful discrimination.
- Do try to avoid receiving unnecessary or questionable material. Immediately delete any inappropriate e-mails or attachments and reply to the sender requesting no further inappropriate material should be sent.
- Be "Legal, Decent, Honest and Truthful"
- Treat e-mail as you would a post card. This is not a secure or private method of communication.
- Report any spam/phishing emails to the College Helpdesk including the email as an attachment.

Internet

- Never view offensive, pornographic or inappropriate material
- Do not use any form of Internet chat that is not authorized by the College
- Do not attempt to interfere with any Internet material or equipment
- Do not use any form of port scanner or any tools designed to find weakness within the
- Internet
- Do not use terminal emulation software
- Use File Transfer Protocol with care. Remember to avoid unnecessary network traffic
- You are not permitted to Buy or Sell using either EBay or any other online auctions during the working day.

Social Media

Hurst is keen to keep abreast of change within the world of electronic and real-time media communication and is aware of and appreciates the power of social media sites and applications, when used appropriately for educational purposes. As a school we are committed to ensuring the safety of our pupils and staff at all times as well as the preservation of our reputation locally, nationally and internationally. As such, pupils and staff must not:

- Put themselves into a position where anything posted might bring the College into disrepute.
- Represent their own personal views as those of Hurst on any social media sites.
- Post any narrative that could be considered either implicitly or explicitly as insulting, threatening, harassing, illegal, abusive, obscene, defamatory, slanderous, or hostile towards any individual or Hurst.
- Discuss or post personal information about other pupils or members of staff at Hurst, including phone numbers, email addresses or any confidential information.
- Post any material that compromises the rights of any Hurst pupil, or member of staff of Hurst entity, including privacy, intellectual property, or publication rights.
- Allow any other individual or entity to use your identification for posting or viewing comments.
- Post comments under multiple names or using another person's name.

Staff must not have current pupils or former pupils under the age of 18 as 'friends' on any personal social media account.

Staff should not add any students, over the age of 18 years, who have left the school, until they have departed for a minimum of two years.

Facebook should not be used by any person under the age of 13. All Prep School pupils are therefore unable to access Facebook on the school network; and they are also discouraged from doing so through private networks before they turn 13.

Procurement and Installation of Hardware & Software

No item of hardware or software may be purchased and / or installed onto a College computer without prior approval of the College Network Manager.

Computers and mobile devices are audited on a monthly basis. Any unauthorized software found on College computers or mobile devices will be investigated and in most cases will be immediately removed. Infringement of copyright is a most serious matter, which could result in disciplinary action being taken.

Use of private computers and BYOD on our network

When connecting your private computers, or mobile devices to our network you are reminded that you must still comply with this Acceptable use Policy.

Agreement

Your use of the College IT facilities and networks is restricted to educational purposes only, such as those, which are consequent upon the teaching, study, research, administration or related activity occasioned by the employment or course of study with the College.

IT Acceptable Usage Policy – Additional information (staff only)

(Reviewer: Dan Higgins; Aug 2023)

This policy forms part of your contract of employment.

Introduction: This policy sets out the requirements with which you must comply when using the College's IT services. Failure to comply with this policy will constitute a disciplinary offence and will be dealt with under the College's Disciplinary Procedure.
Property: You should treat any property belonging to the College with respect and reasonable care, and report any faults or breakages. You are responsible for meeting the cost of any uninsured loss or damage to College property issued to you. You should not use the College's IT services unless you are competent to do so and should ask for training if you need it.
Information: You must ensure confidentiality and responsible use of all College information and materials. Confidential information includes without limitation all information (relating to the College, staff, pupils and their parents or guardians and governors) which is not readily ascertainable other than to persons employed by or holding office with the College and any information in respect of which the College owes an obligation of confidentiality to any third party.
Viruses: You should be aware of the potential damage that can be caused by computer viruses. You must not introduce or operate any programmes or data (including computer games) or open suspicious e-mails which have not first been checked by the College for viruses.
Passwords: Passwords protect the College's network and computer system. They should be changed termly. They should not be obvious, for example a family name or birthdays. You should not let anyone else know your password. If you believe that someone knows your password you must change it immediately. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information which you are not authorised to access.
Leaving workstations: If you leave your workstation for any period of time you should take appropriate action and, in particular, you should log off and/or set your screen saver with an appropriate password. All workstations will automatically lock after 15mins of no activity.

Internet
Personal use: The College permits the incidental use of the internet so long as it is kept to a minimum and takes place substantially out of normal working hours. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. If the College discovers that excessive periods of time have been spent on the internet provided by the College either in or outside working hours, disciplinary action may be taken and internet access may be withdrawn.
Downloading: Downloading of any software programmes, which are not specifically related to your job, is prohibited. All requests for software to run on College devices should be made through the IT dept.
Unsuitable material: Viewing, retrieving or downloading of pornographic material, or any other material which the College believes is unsuitable, at any time, is strictly prohibited and constitutes gross misconduct.
Contracts: You are not permitted to enter into any contract or subscription on the internet on behalf the College, without specific permission from the CFO.

E-mail (also see Email Communication Guidance policy)
Personal use: The College permits the incidental use of its email systems to send personal emails as long as such use is kept to a minimum and takes place substantially out of normal working hours. Personal emails should be labelled 'personal' in the subject header. Use must not interfere with

work commitments. Personal use is a privilege and not a right. If the College discovers that you have breached these requirements, disciplinary action may be taken.

Status: E-mail should be treated in the same way as any other form of written communication. Anything that is written in an e-mail is treated in the same way as any form of writing. You should not include anything in an e-mail which is not appropriate to be published generally.

Inappropriate use: Any e-mail message which is abusive, discriminatory on grounds of sex, marital or civil partnership status, race, disability, age, sexual orientation or religious belief (or otherwise contrary to our Equal Opportunities Policy), or defamatory is not permitted. Use of the e-mail system in this way constitutes gross misconduct. The College will take no responsibility for any offence caused by you as a result of downloading, viewing or forwarding inappropriate e-mails.

Legal proceedings: You should be aware that e-mails are disclosable as evidence in court proceedings and even if they are deleted, a copy may exist on a back-up system or other storage area.

Jokes: Trivial messages and jokes should not be sent or forwarded to the e-mail system. Not only could these cause distress to recipients (if inappropriate) but could also cause the College's IT system to suffer delays and/or damage.

Contracts: Contractual commitments via an e-mail correspondence are not allowed without prior authorisation of the Bursar.

Disclaimer: All correspondence by e-mail should contain the College's disclaimer.

Monitoring: The College regularly monitors the use of the internet and e-mail systems to check that the use is in accordance with this policy. If it is discovered that any of the systems are being abused or that the terms of this policy are being infringed, disciplinary action may be taken which could result in your dismissal.

Social media

Introduction: The College recognises that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, LinkedIn, Twitter, and all other internet postings including blogs and wikis. It is also a valuable educational tool.

Purpose: This policy applies to the use of social media for College and your own personal purposes, whether during normal working hours or in your personal time. Its purpose is to help staff avoid the potential pitfalls of sharing information on such social media sites and should be read in conjunction with the Acceptable Use Policy for pupils.

IT facilities: The policy applies regardless of whether the social media is accessed using the College's IT facilities and equipment or your personal equipment.

Personal use: The College permits the incidental use of social media so long as it is kept to a minimum and takes place substantially out of normal working hours. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. If the College discovers that excessive periods of time have been spent on social media disciplinary action may be taken.

Guiding principles: Staff are required to behave responsibly at all times and adhere to the following principles:

- Use of social media, other than for specific College purposes, should be minimized whether on a College provided device, personal laptop or mobile phone, during College hours.
- Staff should not be "friends" with pupils on any personal social media account. Depending on the circumstances, it may also be inappropriate to add parents as friends too.
- In circumstances where social media platforms are used for communications with pupils, there must be at least two members of staff as part of any group. Staff must also be the owners/admin of the group.

- You must be mindful of how you present yourself and the College on such media.
- Staff are entitled to a social life like anyone else. However, the extra-curricular life of an employee at the College has professional consequences and this must be considered at all times when sharing personal information.
- You should always represent your own views and must not allude to other people's personal views in your internet posts.
- When writing an internet post, you should consider whether the contents would be more appropriate in a private message. While you may have strict privacy controls in place, information could still be shared by others. It is always sensible to consider that any information posted may not remain private.
- You should protect your privacy and that of others by omitting personal information from internet posts such as names, e-mail addresses, home or work addresses, phone numbers or other personal information.
- You should familiarise yourself with the privacy settings of any social media you use and ensure that public access is restricted. If you are not clear about how to restrict access, you should regard all your information as publicly available and behave accordingly.
- You must not post anything that may offend, insult or humiliate others, particularly on the basis of their sex, age, race, colour, national origin, religion, or belief, sexual orientation, disability, marital status, pregnancy or maternity.
- You must not post anything that could be interpreted as threatening, intimidating or abusive. Offensive posts or messages may be construed as cyber-bullying.
- You must not post disparaging or derogatory remarks about the College or its Governors, staff volunteers, pupils or parents.
- You must not use social media in a way which could constitute a breach of any policies contained in this Staff Handbook.

Removing postings: You may be required to remove internet postings which are deemed to constitute a breach of this policy. If you fail to remove postings, this could result in disciplinary action.
Breach: A breach of this policy may be treated as misconduct and could result in disciplinary action including in serious cases, dismissal.
Monitoring: The College regularly monitors the use of the internet, social media and e-mail systems to check that the use is in accordance with this policy. If it is discovered that any of the systems are being abused and/or that the terms of this policy are being infringed, disciplinary action may be taken which could result in your dismissal.

Mobile Device usage
Introduction: This policy sets out the requirements with which you must comply when using any mobile device owned by the College.
Property: You should treat any property belonging to the College with respect and reasonable care and report any faults or breakages immediately. You are responsible for meeting the cost of any uninsured loss or damage to College property issued to you. You should not use the College's devices unless you are competent to do so and should ask for training if you need it.
Personal use: The College permits the use of college-owned tablets and laptops for personal use out of normal working hours provided that the College's E-mail, Internet & Social Media Policy is complied with at all times. Personal use is a privilege and not a right.
Downloading: You should be aware of the potential damage that can be caused by computer viruses. You must not introduce or operate any programmes or data (including computer games) or open suspicious e-mails which have not first been checked by the College for viruses.

Loss and Damage: The College's insurance cover has a high policy excess and for this reason there is no compensation available in the event that machines, or parts thereof are lost, stolen or damaged. You are responsible for any loss or damage to a College laptop, of parts thereof in your charge, however caused, if there has been evident carelessness and particularly in circumstances where a device, or parts thereof are damaged or stolen having been left unattended. If a device, or parts thereof are damaged, lost or stolen, the College reserves the right to deduct appropriate amounts by reasonable instalments from salary to cover repair or replacement costs.
Audit and Checking: College devices are subject to exactly the same audit and checking routines as are applied to all desktop machines in the school. You may therefore be required from time to time to return the device and associated equipment to the IT Department in order for these checks to be carried out. Data stored on the device may be viewed on these occasions.

Mobile Device Policy

(Reviewer Dan Higgins: Aug 2023)

Hurst is committed to providing the best access to the curriculum for all its pupils. The use of mobile devices has been identified as being beneficial for children in the Senior School, over the previously provided iPad in the Prep School. This policy therefore sets out the terms by which those using such devices should operate.

The term 'Surface Pro' refer to school provided devices. The term 'other device' refers to pupils own mobile devices. The term 'mobile device' is generic and relates to both.

Eligibility for use
This policy exists for pupils where Surface Pros are provided as part of their curriculum, as well as elsewhere in the school where mobile devices are recommended but are not compulsory. For pupils with specific learning difficulties, particularly dyslexia the use of mobile devices in lessons and during exams, once practice is established, continues to be encouraged. Pupils may use a mobile device following a recommendation by the Head of Learning Support and approval by the Head of Senior, Head of Prep and Pre/Prep.
Provision of mobile devices
Surface Pros will be provided by the school from Year 7 -11. All other mobile devices are to be provided by parents. All should have a proper keyboard to enable touch-typing. The ability to touch type should be encouraged and taught where possible for any child using a mobile device in school.
Charging
Ideally all mobile devices should be charged at home or in the boarding environments in the evenings. When not in use they should be put on standby or switched off, in order to conserve power. If the device loses power during the school day, the pupil should use pen and paper. They may not be connected to wall sockets at school without permission from a member of staff.
Safety and Security
During school breaks, or when the pupil is elsewhere (eg at games), mobile devices should be stored securely within the pupil's study, either in a locked drawer or left at the pupil's risk within their study room. For insurance and warranty purposes Surface Pros must be carried around the campus in the cases provided. While the school will do what it can to prevent damage or loss to any device, we cannot be held responsible for devices not suitably protected or left unattended, and recommend that parents ensure the device is covered by their own household insurance. School owned mobile devices will be centrally managed to ensure appropriate use. Parents should install controls on any other laptop to prevent the pupil accessing inappropriate sites, either deliberately or accidentally. Improper use of any mobile device, or the omission of appropriate filters, will result in the removal

of its use in school. We recommend that the pupil have a password for their device, in order to protect privacy and work. This should be set to be active immediately that the device is closed down.

School Work Completed on mobile devices

Mobile devices will be used as prescribed by teaching staff, for longer or extended written work. Work completed on mobile devices should be saved and either printed out at home, or emailed, and returned to the subject teacher for marking. The marked work will be returned to the pupil who should stick it into their book. Parents should refrain from amending work brought home on the device as this prevents staff from accurately assessing a pupil's attainment (which informs future teaching).

Homework

Where appropriate, homework may be done on the mobile device. However, as noted for classroom use, some pieces of homework cannot be done successfully on the device.

Pupil Use

Mobile Devices are to be used in school as prescribed by teaching staff. Where appropriate they should be used for word processing, Internet searches and other applications.

All necessary and relevant software will be installed on the devices. Other software that helps pupils may be installed for use at school or home, but only with prior agreement.

Pupils using mobile devices may type work into their device as an alternative to writing it into books or onto sheets. Worksheets specially designed for mobile device use are not provided.

Some work is not appropriate for mobile device use (eg map work, maths) and the pupils must use exercise books, as directed by the teacher.

The pupil may use the spellcheck and grammar functions on their device (except in discrete spelling and grammar exercises). During any assessment or test/exam the spellcheck and grammar function must be disabled. School mobile devices may be provided for formal exams.

The pupil may keep lists of subject-specific technical words on the device and may use these as required during lessons. During assessments or tests/exams these lists must be inaccessible.

In IT lessons, the pupil will use a school computer, the same as the rest of the class.

The pupil may only connect the device to the school network via Wi-Fi or cable using their given login. Any contravention of this will result in the removal of the mobile device's use in school.

Activities other than school work are not permitted on mobile devices used in school. Parents should remove games software installed as part of the operating system.

Pupils must regularly save and backup their work both locally on the device, in the cloud, and/or to the school fileservers.

Improper Use

We reserve the right to remove mobile device use from any pupil who does not comply with required use. This may be for the remainder of a lesson, for a fixed temporary period, or permanently, at the school's discretion.

MOBILE DEVICE AGREEMENT (reference)

Pupil Name: *(Please print)*	Year Group:

In this agreement, 'we', 'us' and 'our' means Hurst College and 'I', 'you', 'your', 'user' means the pupil and parent/guardian. The 'property' is a Surface Pro tablet, keyboard and charging unit owned by Hurst College with the following serial number:

Serial Number:

Please read through this agreement which summarises the commitment the school is making to its pupils and to you as parents/guardians. It also outlines the commitment that will be needed from home to make this new scheme work.

When you have read these sections please sign and return this agreement no later than the first day of term. Pupils, when issued the mobile device, will be asked to sign an Acceptable Use Policy (AUP).

Please note that this form must be completed and returned to the College before the device will be issued.

Hurst College will:

- Provide a mobile device for the use of your son/daughter for educational purposes based on a lease arrangement. The provision will be reviewed at the end of each 3 year period. The school will be the lessee.
- Ensure that the device is working and loaded with appropriate software when handed over and offer technical support as is appropriate during term time.
- Make sure that the device is covered by insurance whilst at school, on the direct journey to and from school, and on school trips within the UK, providing reasonable care is taken to prevent loss or damage.
- Give pupils an introduction to using and caring for the mobile device and the software.
- Provide first line technical support and warranty services to pupils (and parents) through the warranty

Users undertake to:-

- Make every effort to protect the computer against virus infection and malware or other undesirable software.
- Ensure that your son/daughter understands how to care for and protect the device in accordance with the manufacturer's instructions and relevant College IT policies.
- Ensure that the device is returned in good condition if the pupil leaves the school, or at any other time upon the request of a member of the IT staff.
- Make sure the device is not used for any illegal, immoral and/or anti-social purpose.
- Report any loss or damage (including any accidental loss or damage) immediately to the College or in person to the IT department, returning the device if requested.
- Meet the cost of any uninsured losses and pay an excess of £150 for any claims made.
- If the device is stolen you must immediately report it to the police and get a crime reference number. Also to report this to the Network Manager during term-time and/or throughout any school holidays.
- Inform the College of any change of home location for the laptop.
- Abide by the sections of the College Acceptable Use Policy (AUP) relating to device use and sign to confirm this acceptance.

As a user I will:

- Look after my Surface Pro, keyboard and charger very carefully all of the time, not leaving it unattended or on show.

- Bring the mobile device to school every day fully charged and ready for use.
- Always carry it around in the proper case/bag so that it is fully protected.
- Take care when it is transported that it is as secure as possible.
- Make sure that the mobile device is not subject to careless or malicious damage by myself or others.
- Keep my password and other authentication information a secret from others and ensure it is locked if I walk away.
- Take reasonable precautions to prevent the introduction of computer viruses.
- Not decorate or customise the mobile device and not to allow it to be subject to graffiti.

- Look after my own Health and Safety when using the device.
- Report any e-safety concerns to the Mrs Stoneley, Director of Safeguarding / tutor / HoM when they become apparent (this includes cyber-bullying and harassment etc.)

Hurst College is not responsible for and will not accept liability for:-

- Crimes against the computer or user covered by the Computer Misuse Act and amending legislation.
- Loss of personal data.
- Home banking/financial transaction issues.
- Use for illegal or immoral purposes.
- The first £150 of any insurance claim

The mobile device (plus software and accessories) remains the property of Hurst College, even when it is at your home. It will be loaned to the named person for the duration of the period in which you are a pupil at Hurst College.

You will be issued with:

- Surface Pro
- Detachable keyboard
- Protective named case
- A charging unit which must be returned with the device. A charge will apply for lost or damaged chargers

There may be occasions when a mobile device needs to be returned to the school and/or for repair, and it may be necessary to completely remove all information on the device. We would therefore recommend regular backing-up of your work and data before handing it to technical staff.

The above terms and conditions may change from time to time, parents/guardians and users are expected to accept these changes as notified.

We have read the school's mobile device policy and agree to abide by the requirements. We understand that any misuse of the mobile device at school will result in the device use being withdrawn. This may be for a fixed period or permanently, depending on the situation and at the school's discretion.

Signed: (Parent) ____
Signed: (Child) ____
Date: ____

STAFF SURFACE PRO AGREEMENT (for reference)

In this agreement, ‘we’, ‘us’, 'our’ and 'the College' means Hurstpierpoint College Ltd and ‘I’, ‘you’, ‘your’, ‘user’ means the member of staff. The ‘property’ is a Surface Pro tablet device and charging unit owned by the College with the following serial number:

Staff name:

Please read through this agreement which summarises the commitment the College is making to you. It also outlines the commitment that will be needed from you to make this scheme work.

When you have read these sections please (digitally) sign and return this agreement no later than Monday 10th September.

Staff when called forward for issue of the device will be asked to digitally sign an Acceptable Use Policy (AUP) too.

Please note that this form must be completed and returned to the College and an AUP completed before use of the device.

Agreement.
The College will:

- Provide a Surface Pro tablet for the use of you for educational purposes. The provision will be reviewed annually.
- Ensure that the device is working and loaded with appropriate software when handed over and offer technical support as is appropriate during term time.
- Ensure that the device is covered by insurance against theft or damage, providing reasonable care is taken and subject to certain exceptions - including loss if left unattended in a public place or in a vehicle.
- Give an introduction to using and caring for the device and the relevant software.
- Provide first line technical support and warranty services to you through the provided warranty.

Users undertake to:-

- Make every effort to protect the computer against virus infection and malware or other undesirable software.
- Ensure that you understand how to care for and protect the device in accordance with the manufacturer’s instructions and relevant College IT policies.
- Ensure that the device is returned in good condition if you leave the school, or at any other time upon the request of a member of the IT staff.
- Make sure the device is not used for any illegal, immoral and/or anti-social purpose.
- Report any loss or damage (including any accidental loss or damage) immediately to the Network Manager, or in person to the IT department, returning the device if requested.
- Meet the cost of any uninsured losses and pay an excess of £150 for any claims made.
- If the device is stolen you must immediately report it to the police and get a crime reference number. Also to report this to the Network Manager during term-time and during school holidays.
- Inform the College of any change of home location for the device.

- Abide by the sections of the College Acceptable Use Policy (AUP) relating to device use and sign to confirm this acceptance.

As a user I will:

- Look after my device and charger very carefully all of the time, not leaving it unattended or on show.
- Bring the device to school every day fully charged and ready for use.
- Always carry it around in the proper case so that it is fully protected.
- Take care when it is transported that it is as secure as possible.
- Not leave it unattended in a public place or in a vehicle (except in the locked boot of a car).
- Make sure that the device is not subject to careless or malicious damage by myself or others.

- Keep my password and other authentication information a secret from others and ensure it is locked if I walk away.
- Take reasonable precautions to prevent the introduction of computer viruses.
- Not decorate or customise the device and not to allow it to be subject to graffiti.
- Look after my own Health and Safety when using the device.
- Report any e-safety concerns to the relevant member of SMT (this includes cyber-bullying and harassment etc.)

The College is not responsible for and will not accept liability for:-

- Crimes against the computer or user covered by the Computer Misuse Act and amending legislation.
- Loss of personal data.
- Home banking/financial transaction issues.
- Use for illegal or immoral purposes.
- Uninsured losses and the first £150 of any insurance claim

The device (plus software and accessories) remains the property of the College, even when it is at your home. It will be loaned to the named person for the duration of the period in which you are a member of staff at the College. It is possible that, after a period of time your device will be replaced, and a replacement one issued.

You will be issued with:

- Surface Pro
- Detachable keyboard
- A charging unit which must be returned with the device. A charge will apply for lost or damaged chargers
- A suitable protective case for transportation

There may be occasions when a device needs to be returned to the school and/or for repair, and it may be necessary to completely remove all information on the device. We would therefore recommend regular backing-up of your work and data before handing it to technical staff.

The above terms and conditions may change from time to time, and users are expected to accept these changes as notified. A full wording of these amended terms and conditions can be found on GRS.

User Agreement

I, , agree to abide by these terms in my use and care of the device.

Signature: Date:

Hurst E-Safety Policy
(Reviewer: Simon Hilliard / Dan Higgins Aug 2023)

This E-safety policy uses the following terms unless otherwise stated:

USERS: refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the College, including contractors.

PARENTS: any adult with a legal responsibility for the child/young person outside the College e.g. parent/guardian/carer
COLLEGE: any College business or activity conducted on or off the College site, e.g. visits, conferences, school trips etc.
WIDER SCHOOL COMMUNITY: students, staff, governing body, parents.

Safeguarding is a serious matter and at Hurstpierpoint College we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as E-safety, is an area that is constantly evolving and, as such, this policy will be reviewed on annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is two-fold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available to view on the the College website; upon review. A copy of this policy and the Students Acceptable Use Policy will also be available on the Parent Portal for pupils and parents to read and acknowledge. On acceptance of the terms and conditions, students will be permitted access to school technology, including the Internet.

Policy Governance
The governing body is accountable for ensuring that the College has effective policies and procedures in place; as such they will:

Review this policy at least annually and in response to any serious e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

The College has a named E-Safety Governor, currently Mrs Fran Hampton. The role of the E-Safety Governor is to:

- Keep up to date with emerging risks and threats through technology use
- Receive regular updates from the Director of Safeguarding with regard to training, identified risks and any incidents.
- Update the Safeguarding committee of any E-safety incidents or measures that need to be implemented. To include :
    - Advising changes to the E-safety policy
    - Establishing effectiveness (or not) of E-safety training and awareness at the school.
    - Recommending further initiatives for E-safety training and awareness at the school.

The Head of College, reporting to the governing body, has overall responsibility for E-safety within the College. The day to day management of this is delegated to the Director of Safeguarding. The Head of College will ensure that:

- E-safety training throughout the school is planned and up to date and appropriate to the recipient, ie. Students, all staff, SMT/SLT, governing body and parents.
- The designated safeguarding officer has appropriate CPD in order to undertake their day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

The day to day duty of the E-safety Officer is devolved to Simon Hilliard (Director of Safeguarding). The E-safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Head of College and staff.
- Advise the Head of College and governing body on e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with IT department, Chief Operating Officer and the technical support team, as required.
- Retain responsibility that any e-safety incidents be recorded on CPOMS and ensure that staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. internet filtering software, behaviour management software) are fit for purpose through liaison with Chief Operating Officer.
- Make themselves aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function.

The IT technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
- Anti- virus is fit for purpose, up to date and applied to all capable devices
- Windows updates are regularly monitored and devices updated as appropriate
- Any e-safety technical solutions, such as Internet filtering, are operating correctly
- Filtering levels are applied appropriately and according to the age of the user
- Categories of use are discussed and agreed with the E-safety officer
- Passwords are applied correctly to all users, regardless of age. Passwords are changed every 120 days and should contain a minimum of 10 characters, include a Capital; 1 numeric, and 1 special character/symbol. The system will not accept anyone of your previous 5 passwords to be reused.
- The I.T. System Administration password is to be changed on a regular basis.

- The filtering system protects the children, as far as is practically possible, from the threat of Radicalisation, paying due regard to the Prevent Duty.

All Staff are to ensure that:

- All details within this policy are understood. Anything that is not should be brought to the attention of the E-safety officer.
- Any E-safety incident is reported to the E-safety officer.
- They fully understand the reporting process.

All Students

- The boundaries of use of IT equipment and services in this school are given in the student Acceptable Use Policy. Any deviation or misuse of IT equipment or services will be dealt with by the school's Behaviour and Discipline Policy.
- E-safety is embedded into our curriculum.
- Students will be given the appropriate advice and guidance by staff. Similarly, all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. The College will keep parents up to date with new and emerging e-safety risks, as appropriate, and will involve parents in strategies to ensure that students are empowered to stay safe.

Parents must also understand that the College needs to have rules in place to ensure that their child can be properly safeguarded. As such, parents will be expected to acknowledge the IT Acceptable use Policy before any access can be granted to school IT equipment or services.

Technology

The College uses a range of devices including P.C.'s, laptops, and iPads. We also support BYOD via our Wi-Fi networks. In order to safeguard our students, and in order to prevent loss of personal data, we employ the following assistive technology:

Internet Filtering

Smoothwall software prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites. (Appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner). The Chief Operating Officer, E-safety officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the DSL.

Email Filtering

Microsoft Exchange software prevents any infected email being sent from the school or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption

All school devices that hold personal data (as defined by the Data protection Act 1998) are encrypted. No data is to leave the school on an unencrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptops or USB key drives) is to be brought to the attention of Chief Operating Officer and the E-safety Officer, immediately.

Passwords
All staff and students will be unable to access any device without a unique username and password. Staff and student passwords change on a regular basis or, if there has been a compromise, whichever is sooner. The Network Manager will be responsible for ensuring that passwords are changed.
The school actively discourages devices which are not password enabled.

Anti Virus
All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. The Network Manager is responsible for this.

Use of Images Policy

(Reviewer: Darren Carpenter; September 2023)

Policy on use of Images

Introduction
The Data Protection Act 2018 not only governs the way in which we process information about people but also the way we handle images of people. These notes have been produced to help you ensure that we comply with the law when images of clearly identifiable people are being used. These images may appear in any or all of the following formats:

- paper publications
- photographs
- videos
- webcams
- the internet
- multimedia messaging service (MMS) mobile phones
- Images for College publications

The College does seek consent from parents for the use of images of our pupils, and it is reasonably assumed that the College marketing team and other College staff will take images from time to time, where appropriate and in a suitable manner for College publications, for example the College website, Hurst Johnian, etc. It should be remembered, however, that taking photographs or images can be a delicate matter and this should approached with due care and attention to context, situation, the wishes of the person of who the image is being taken. For more information, please refer to the Code of Conduct.

Pupil use of Mobile phones policy

(Reviewed: Dominic Mott August 2021)

The College aims to encourage the responsible use of mobile phones and expects pupils to use their devices in a way that is appropriate not only to the school environment but also to the age of the pupil. As such, the rules below are adapted according to the year group, with older students receiving more flexibility to take responsibility for their mobile phone usage.

Overview
Mobile phones are helpful for keeping in touch, as an educational resource and for staying safe. They provide direct contact to key people in a pupil’s life, and at times provide a necessary

reassurance due to their ease of access. Pupils at Hurst are encouraged to employ mobile phones in moderation, in order to communicate with their families and friends in a manner that promotes positive relationships. They are simultaneously discouraged from their inappropriate use during the academic day and at other times. Pupils are educated about how to stay safe online, the School's IT Acceptable Use Policy and on the negative impact of excessive screen time.

When connected to the school wifi, the use of mobile phones falls under the College's IT Acceptable Use Policy to which all pupils must agree and with which they must comply. Mobile phones (incorporating cameras) that transmit images may not be used in such a way as to compromise the safety of others. Any unacceptable use of the internet via personal mobile phones will be dealt with in accordance with the School's Behaviour and Discipline Policy. If needed, pupils may request to use the School phone. Parents wishing to contact their children in an emergency should always telephone the School office and a message will be relayed promptly.

Under the 'Searching, Screening and confiscation' guidelines published by the DfE in January 2018, the School reserves the right to confiscate and/or search a pupil's mobile phone for a specified period of time if the pupil is found to be in breach of this policy or if there is 'good reason' to do so. In determining a 'good reason' to examine or erase the data or files the staff member should reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules. In such cases, the School may examine any data or files on the device. The school may also delete data or files if there is a good reason to do so, unless the School is going to give the device to the police. Under government guidelines there is no need to have parental consent to search through a young person's mobile phone if it has been seized in a lawful 'without consent' search and is prohibited by the school rules or is reasonably suspected of being, or being likely to be, used to commit an offence or cause personal injury or damage to property.

The pupil may also be prevented from bringing a mobile phone into the School temporarily or permanently at sole discretion of the Head of College or the Head of Junior Prep School and the Head of Senior Prep School. The School does not accept any responsibility for the theft, loss of, or damage to, mobile phones brought onto School premises.

Prep School Mobile Phone Policy

No child in Years Reception to Year 2 is allowed to bring a mobile phone into School.

All Prep School pupils are forbidden to use or carry mobile phones within school hours for any purpose, including texting, phoning, taking still or moving images, checking the time, using Bluetooth, using as a calculator or surfing the internet. Phones must be handed into the school office upon arrival at school.

Years 3 to 8 in the Prep School may take phones with them if they are going to an away match or similar event and will be picked up from there and not return to school. In such cases the teacher/coach must be informed and the phone must not be used without the permission of the member of staff in charge and will only be used to contact the pupils parent or guardian.

Senior School Mobile Phone Policy

Shell, Remove and Vth pupils are forbidden to use or carry mobile phones within school hours for any purpose, including texting, phoning, taking still or moving images, checking the time, using Bluetooth, using as a calculator or accessing the internet. Day pupils who bring a mobile phone into school must hand in their mobile phone to their HoM upon arrival at school and may collect it at the end of the school day. Boarders wishing to use their phones in the evening are given a window to contact friends/family, but should hand their phone back in to the HoM before bed.

Pupils in the Fifth Form and above may bring their mobile phone into school but these should not be seen or used outside of House, unless permission has been granted by the teacher. Pupils are encouraged to only use phones in breaks/social times and no phones should be seen or used in the Dining Hall, including the queue in the Cloisters. Pupils should avoid using mobile phones whilst walking around the campus. Any pupil found in breach of these rules may have their mobile phone confiscated by a member of staff, who will pass it on to the Head of Senior School. The pupil may collect their phone from the Head of Senior School from 6pm who will speak to them about appropriate usage. Repeat offenders may have their phones removed for longer periods of time.