ICT ACCEPTABLE USE POLICY

Table of Contents

Reviewed by:	O Hickmott – Technical Director	**Date:** 20/06/2022
Last reviewed on:	June 2022	
Next review due by:	June 2023	
Ratification by Governors on:	July 2022	

1. INTRODUCTION AND AIMS

Herne Bay High School recognises Information and communications technology (ICT) as integral to the success of our school, and a critical resource for teaching and learning, and supporting the pastoral and administrative functions of the school. We encourage the use of technology to enhance skills and promote achievement.

However, the accessible and global nature of ICT our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective use of ICT
- Ensure school technology remains uncompromised and relevant

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be subject to disciplinary action. This could include formal warnings, suspension, potential dismissal, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of law enforcement.

2. RELEVANT LEGISLATION AND GUIDANCE

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2022
- Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021
- The Digital Economy Act 2017
- Copyright, Design and Patents Act 1988
- Sexual Offences Act 2003
- Obscene Publications Act 1959 and 1964
- Communications Act 2003
- Malicious Communications Act 1988 (section 1)
- Protection from Harassment Act 1997
- Racial and Religious Hatred Act 2006
- Criminal Justice Act 2003

3. DEFINITIONS

- ICT facilities : includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software,

websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service.

- Users : anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.
- Personal use : any use or activity not directly related to the users' employment, study or purpose
- Authorised personnel : employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities.
- Materials : files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.
- Antivirus : Software designed to detect, stop and remove malicious software and viruses.
- Cloud : Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
- Cyber attack : An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
- Cyber incident : Where the security of your system or service has been breached.
- Cyber security : The protection of your devices, services and networks (and the information they contain) from theft or damage.
- Firewall : Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
- Hacker : Someone with some computer skills who uses them to break into computers, systems and networks.
- Malware : Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
- Patching : Updating firmware or software to improve security and/or enhance functionality.
- Phishing : Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
- Ransomware : Malicious software that stops you from using your data or systems until you make a payment.
- Social engineering : Manipulating people into giving information or carrying out specific actions that an attacker can use.
- Spear-phishing : A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
- Trojan : A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
- Two-factor/multi-factor authentication : Using 2 or more different components to verify a user's identity.
- Virus : Programs designed to self-replicate and infect legitimate software programs or systems.
- Virtual Private Network (VPN) : An encrypted network which allows remote users to connect securely.

4. UNACCEPTABLE USE

The following is considered unacceptable use of school ICT facilities, by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to access, create, store or distribute any material which are illegal or potentially unlawful, promote unlawful discrimination, offensive, obscene, racist, defamatory, abusive, intimidating, insulting, indecent, harassing or otherwise covered by the Racial and Religious Hatred Act 2006, Criminal Justice Act 2003, Sexual Offences Act 2003, Communications Act 2003, The Computer Misuse Act 1990, Malicious Communications Act 1988, Copyright, Design and Patents Act 1988, Public Order Act 1986, Obscene Publications Act 1959 and 1964, Protection from Harassment Act 1997 and Criminal Justice and Immigration Act 2008.
- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to capture and / or publish images of others without their express consent
- Breaching the school's policies or procedures

- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to, or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Promoting a private business or political party, unless directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way
- Engaging in content or conduct that may compromise professional responsibilities

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Principal, Data Protection Officer or Technical Director will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 EXCEPTIONS FROM UNACCEPTABLE USE

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Principal's discretion.

4.2 SANCTIONS

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on behaviour, discipline, conduct and anti-fraud. Policies are available on the school website or in Microsoft Teams.

5. STAFF (INCLUDING GOVERNORS, VOLUNTEERS, AND CONTRACTORS)

5.1 ACCESS TO SCHOOL ICT FACILITIES AND MATERIALS

The school's Technical Director manages access to school ICT facilities, accounts and materials for staff. This includes, but is not limited to:

- Desktops, laptops, tablets, phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the school's technical support team.

5.2 USE OF PHONES, EMAIL AND INSTANT MESSAGING

The school provides each member of staff with a Microsoft 365 account and email address.

This account should be used for work purposes only. Staff must enable multi-factor authentication on their accounts to enable access outside of the school.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email and instant messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email and instant messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the Data Protection Officer immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones or phone lines provided by the school to conduct all work-related business.

School phone lines must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

The school can record in-coming and out-going phone conversations.

If you record calls, callers must be made aware that the conversation is being recorded and the reasons for doing so.

All recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

5.3 PERSONAL USE

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Technical Director may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contracted hours
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.7). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with section 4 of this policy.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.2) to protect themselves online and avoid compromising their professional integrity.

5.4 PERSONAL SOCIAL MEDIA ACCOUNTS

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times. Staff should take care not to engage in any online activity that may compromise their professional responsibilities.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.5 REMOTE ACCESS

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the Technical Director may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

The school's data protection and data retention policy is located on the school website.

5.6 SCHOOL SOCIAL MEDIA ACCOUNTS

The school has official Facebook and Twitter accounts, managed by the Director of Communications and the Technical Director. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

5.7 MONITORING OF SCHOOL NETWORK AND USE OF ICT FACILITIES

As part of our obligation to comply with Keeping Children Safe in Education and the Prevent Duty, appropriate filters and monitoring are in place. The school is constantly reviewing industry trends to improve filtering and monitoring in accordance with Keeping Children Safe in Education and any other Department for Education and online safety statutory guidance. The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Web activity, including sites visited and search terms
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Ensure effective school and ICT operation
- Safeguard staff and pupils
- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

5.8 INSPECTION AND SERVICING

Any device issued to staff or pupils remains the property of the school at all times, and must be returned at the end of a lease or contractual period, or when requested by the Technical Director or the Principal.

Staff and pupils have a responsibility to protect issued devices from unauthorised access, damage or theft, and must ensure devices are not left unlocked or accessible whilst unattended. Staff and pupils, parents or carers may be liable for repair or replacement costs caused by negligence or abuse.

To ensure security, effective operation and reduce risk of failure or data breach, it is imperative that school owned devices are inspected, maintained and updated on a regular basis. It is the responsibility of the school's Technical Director to ensure effective inspection, update and replacement for ICT facilities. Staff and pupils are required to make issued equipment available upon request.

6. PUPILS

6.1 ACCESS TO SCHOOL ICT FACILITIES AND MATERIALS

The school's Technical Director manages access to school ICT facilities, accounts and materials for pupils. This includes, but is not limited to:

- Desktops, laptops, tablets and other devices
- Access permissions for certain programmes or files

Pupils will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

The school will ensure pupils have good access to ICT facilities to enhance their learning and will, in return, expect pupils to be responsible users.

6.2 SEARCH AND DELETION

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

6.3 UNACCEPTABLE USE OF ICT OUTSIDE OF SCHOOL

The school will sanction pupils, in line with its behaviour and discipline policy, if a pupil engages in any of the following at any time (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities

- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. PARENTS

7.1 ACCESS TO SCHOOL ICT FACILITIES AND MATERIALS

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with the school in an official capacity (for instance, as a volunteer or as a member of the Governing Body) may be granted an appropriate level of access or be permitted to use the school's facilities at the Principal's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 COMMUNICATING WITH OR ABOUT THE SCHOOL ONLINE

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses the following channels:

- Our official Facebook page
- Our official Twitter account
- Our official website
- Our school mobile applications
- Email/text groups for parents (for school announcements and information)

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

Parents must not:

- Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way.
- Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils.
- Upload or share photos or videos on social media of any child other than a child they have parental responsibility for, unless they have written consent of other children's parents/carers

8. DATA SECURITY

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

8.1 PASSWORDS

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

All staff will use a password manager to help them store their passwords securely. Authorised personnel will generate passwords for pupils using a password manager/generator and keep these in a secure location in case pupils lose or forget their passwords.

8.2 SOFTWARE UPDATES, FIREWALLS AND ANTI-VIRUS SOFTWARE

All of the school's ICT systems that support software updates, security updates and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must be configured in this way.

8.3 DATA PROTECTION

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

The school's data protection and data retention policy is located on the school website.

8.4 ACCESS TO FACILITIES AND MATERIALS

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the school's Technical Director.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the school's Technical Director immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

8.5 ENCRYPTION

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the Technical Director.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Technical Director.

9. PROTECTION FROM CYBER ATTACKS

The school will:

- Work with governors and technical support to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:

    - ‘Proportionate’: the school will verify this using a third-party audit, to objectively test that what it has in place is up to scratch
    - Multi-layered: everyone will be clear on what to look out for to keep our systems safe
    - Up-to-date: with a system in place to monitor when the school needs to update its software
    - Regularly reviewed and tested: to make sure the systems are as up to scratch and secure as they can be
- Back up critical data daily and store these backups on cloud-based backup systems
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our technical support team, cloud provider and external technical advisors/auditors
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where available
    - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the technical support team, for example, including how the school will communicate with everyone if communications go down, who will be contacted when, and who will notify Action Fraud of the incident

10. INTERNET ACCESS

The school’s internet bandwidth is designed to cope with the school’s ‘normal’ demands. Bandwidth utilistaion is monitored by the school and under regular review to ensure it is meeting demand, whilst aiding in fault detection and misuse.

All use of the internet from a school owned device (used within school or an external internet connection), or from a personal device connected to the school ICT infrastructure will be monitored and logged in accordance with this policy and our obligation to comply with Keeping Children Safe in Education (September 2022) and the Prevent Duty.

When specific circumstances of abuse warrant it, individual web sessions will be investigated and linked to the relevant user account. Such an investigation may result in action via the school’s Disciplinary Procedure and possibly criminal investigation.

Despite reasonable steps being taken if unsuitable content is discovered this should be reported immediately to a member of staff or the school’s technical support team. Attempts to bypass filtering systems are strictly prohibited and may result in a user’s access being removed.

The school requires all users of the wireless network to log in using their school supplied credentials or a guest pass provided by the school. The school monitors online activity and is able to identify individuals as part of this process.

A reporting system is in place for Designated Safeguarding Leads (DSLs) to monitor online activity and address areas of concern. The school recognises that pupils and staff can access the internet over mobile phone operators cellular connections. Parents are advised to make use of the filtering and monitoring facilities provided by their mobile phone operator on these connections.

11. MONITORING AND REVIEW

The Principal and Technical Director monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed annually and ratified by the school Governing Body.

12. RELATED POLICIES

This policy should be read alongside the school's policies on:

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Remote learning

APPENDIX 1: FACEBOOK CHEAT SHEET FOR STAFF

Don't accept friend requests from pupils on social media

10 RULES FOR SCHOOL STAFF ON FACEBOOK

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

CHECK YOUR PRIVACY SETTINGS

- Change the visibility of your posts and photos to 'Friends only', rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your old posts and photos – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've 'liked', even if your profile settings are private, because this depends on the privacy settings of the original poster
- Google your name to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't search for you by name – go to bit.ly/2zMdVht to find out how to do this
- Remember that some information is always public; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

WHAT TO DO IF…

A PUPIL ADDS YOU ON SOCIAL MEDIA

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages

- Notify the senior leadership team or the Principal about what's happening

A PARENT ADDS YOU ON SOCIAL MEDIA

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

YOU'RE BEING HARASSED ON SOCIAL MEDIA, OR SOMEBODY IS SPREADING SOMETHING OFFENSIVE ABOUT YOU

- Do not retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Pupil ICT Acceptable Use Agreement

School Policy

Herne Bay High School recognises the potential benefits and opportunities that new technologies offer to teaching and learning. We encourage the use of technology to enhance skills and promote achievement. However, the accessible and global nature of the internet and variety of technologies available mean that we are also aware of potential risks and challenges associated with such use. This agreement is intended to implement safeguards within the school and to support learners to identify and manage risks independently.

This agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will ensure pupils have good access to ICT to enhance their learning and will, in return, expect pupils to agree to be responsible users.

Acceptable Use

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will log on to the ICT system using only the provided username and password and I will not make any password known to any other person.
- I will not disclose or share personal information about myself, the school or other members of the school community online.
- I will not use the school system to arrange to meet people that I have communicated with online. Furthermore, the school's position is that a young person should not meet anyone that they have communicated with online, unless they have the agreement of their parent(s)/carer(s) and, if they receive this agreement, then they should take an adult with them and meet that person in a public place.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not attempt to bypass internet filtering approaches, test the weaknesses of the ICT system or undertake deliberate activities that waste staff effort or affect the service for other users.
- I will not use the school ICT systems for personal financial gain, online gaming, gambling, internet shopping.
- I will not use file sharing or video broadcasting, unless I have permission from a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use aggressive, offensive, obscene, defamatory, abusive, intimidating, insulting, indecent, harassing or otherwise objectionable language and I appreciate that others may have different opinions.
- I will not take or distribute still or video images of anyone without their consent.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my personal devices (including but not limited to, mobile phones, tablets, smart watches, USB devices) in school if I have permission from a member of staff. I understand that, if I am permitted to use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. School Rules state 'should a student wish to bring a mobile phone to school, they must turn it off between 8.30 and the end of the school day and must not send or receive calls or messages until they have finished school for the day. Any contravention of this rule could result in the student's phone being taken from them and securely stored until the end of the day or until a parent/carer is available to come in to collect the phone'.
  Note – Herne Bay High School is unable to accept responsibility for any items of value brought into school that are either lost or damaged, such as mobile phones, laptops, tablets, ipods, games consoles, bicycles or money.
- I understand the risks and will not try to create, access, store or transmit any materials which are illegal, potentially unlawful or may cause harm or distress to others, nor will I try to use any methods to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not attempt to do anything that threatens the integrity or security of the school ICT system, including, but not limited to, introducing or creating any form of malicious software.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies.
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that I must not, through my actions whilst using digital communications either at home or school, bring the name of the school into disrepute.
- I understand that the school may enact it's disciplinary approaches against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, internal / external exclusions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

Full name: _____

Signature of student: _____

Signature of parent/carer: _____

Date: _____