Acceptable Use Policy
Norton Canes High School

January 2023

Norton Canes High School

Acceptable Use Policy - Learners and Staff

Produced Date:	**January 2023**
Approved by Governors:	**[Name]**
Review Date:	**[Date]**

Date	Section Amended	Signature

Norton Canes High School			
Position	**Signed**	**Print**	**Date**
Chair of Governors			
Head Teacher			

Contents

1. General Statement

Computers and ICT equipment are provided for the benefit of all in the learning community, and to help deliver improvements in teaching and learning. Access to the facilities is a privilege and not a right. There are some basic rules that staff and learners need to follow, to ensure that everyone in our school community can benefit from these facilities.

2. ICT Equipment

Don't break or damage IT equipment, either on purpose or by being careless. This includes not eating or drinking near the computers. Please notify the ICT department of any damage to equipment or any unusual programmes in place, such as commercial software or a new web browser 'home page'.

You should only install any software or extra hardware (printers, scanners, mice, speakers) if you have first checked with the ICT department. This is particularly important for apps, as they may have wide-ranging permissions that compromise the security of your machine and the ICT network as a whole.

If you are connecting mobile equipment to the network, always ask ICT staff to help so that it is done safely and that your equipment can be virus checked and protected. Please note that if the equipment does not have anti-virus software installed then ICT staff will not add it to the network.

3. Security and Privacy

Use of passwords is designed to keep your data safe online, and ensure that only you have access to your work. It also helps ICT staff track who is using resources and how they are using them.

You should use a strong password, and must not tell anyone else what that password is. If someone else uses your account to break the ICT rules, and you have told them your password, you will be equally responsible for their actions. If you think that someone has tried to access your ICT equipment or shared files inappropriately, please tell ICT immediately. On occasion, it may be necessary for you to divulge your password to ICT staff in order for them to perform maintenance, updates and install software to equipment. Passwords can be reset once completed.

Always lock computers and mobile devices when you are away from your desk or workspace, to prevent others accessing your files and information.

You may have access to shared drives or shared network areas. These are provided to help collaborative working and shared research. Do not abuse these facilities to try to gain access to areas that you should not be looking at. If you find that you are able to see files and content that you don't think you should, please tell ICT staff.

If you have access to confidential or personal information as part of your work, this must be kept only in the designated secure areas and applications. You must not disclose any personal information to anyone who does not have a right to see it.

4. Acceptable use of the Internet

Staff and learners are encouraged to explore the internet and use a range of resources for teaching and learning. This should be done in a responsible way, and with an open-mindedness to new ideas and new ways of thinking.

Rules about internet use apply equally to all staff and learners. This helps to promote shared values within the school, and to promote shared learning.

Use of the internet is monitored to help ensure network security and promote efficient use of the available resources. Unusual volumes of traffic will be noted. If you are using significant internet resources you may be asked to explain how this promotes the school's aims and values.
Network filtering is in place to prevent access to inappropriate sites, and there is keyword logging software that flags certain terms. It will be clear to you if you have 'hit the firewall' by using a search term or location that may be inappropriate, or if your access to a site or resource is blocked. If that happens, please make a note of what you were trying to do at the time, as you may be asked to explain to a teacher or senior manager.

Please notify ICT staff immediately if you access any inappropriate sites by accident, or if you find inappropriate content on a workstation or the internet.

You must use the internet in accordance with UK law. Any illegal use will be dealt with through official channels, which may include the involvement of police if a crime has been committed.

5. The school email system

The school provides an email system to facilitate teaching and learning. It allows staff [and learners] to communicate quickly with one another, and to provide a quick and easy way to deal with outside agencies on any school business.

Anything sent through the school email system may be accessed and viewed by senior leaders if there is a valid reason to do so. The school will directly access email accounts in the course of an appropriately authorised investigation.

Staff should not email school files or documents to personal email accounts. If you are sending a document to yourself to work on at home or at another site, use the school email address or a shared cloud server provided by the school, such as OneDrive.

Use of email may be subject to monitoring for security and/or network management reasons.

Your school email address should only be used for school business, and in connection with teaching and learning. It should not be used for general everyday purposes.

Staff [and learners] should be aware that it is unacceptable to use the email system to send or receive any material that is obscene or defamatory, or to use it to in any way intended to annoy, harass or intimidate another person. Any reporting instances of using email in this way will be dealt with by senior leaders.

6. Email Security

Norton Canes High School has strong email and internet security in place. However there is always the risk that scam, phishing or chain emails may get through this, and be received on your school email

account. Staff and learners need to be aware that not everything sent to your school email account may be what it seems.

Scam or phishing emails may contain content such as viruses, malware and ransomware. Viruses infect your machine and make it harder to use, by example by making you unable to open programs, or changing your default internet log-in page to a scam site. Malware may track information such as your web visits and key strokes, and send this back to the scammer. This may allow them to access your online accounts. Ransomware encrypts files on your machine and locks them down. When you try to open them, you see a ransom demand to have them decrypted and returned to you.

If you receive an unusual or suspicious email, you should not open it. You should delete it from your 'inbox' and your 'delete' box, and notify ICT staff. Please forward suspicious emails to the ICT department. Tell ICT support basic details about the email subject and address, and allow them to investigate.

7. Using ICT equipment away from the school site

You should take care when using or transporting school-issued ICT equipment away from the school site. You will be responsible for taking all due care to ensure that it is kept safe and is not lost or stolen.

You should take additional care if working offsite to ensure that data and information on your machine is not accessed by anyone else. You should use your password and lock the machine if you are away from it for any length of time. Make sure your screen cannot be seen by other people if you are working in a public place.

Any apps or log-ins to school systems should be closed when you are no longer using them. This will ensure that any personal data being accessed is kept safe and secure.

Memory sticks are not secure and are easily mislaid. There are many preferable alternatives to using memory sticks to transfer and access documents away from the school site. This might include using the schools One Drive and school email accounts for storing and accessing documents or data. If there is no alternative to using a memory stick, for example if you do not have internet access at your off-site workplace, then the memory stick must be encrypted.

8. What is unacceptable conduct?

Norton Canes High School aims to encourage positive use of ICT equipment to enhance teaching and learning opportunities. Using the resources and facilities in any way that is not positive and goes against the spirit of this Policy could be considered to be unacceptable.

In particular, all users must be aware that they must not use the school equipment or network to obtain, download, send, print, and display or otherwise transmit or gain access to materials that are unlawful, obscene or abusive or contain other objectionable materials. In addition, any kind of abuse of others is unacceptable. This would include any actions that intend to belittle others based on their race, gender, religion, sexual orientation or other aspects of their chosen social character.

Neither staff nor learners should use the ICT facilities for commercial activities or money-making schemes. The only exception to this could relate to approved fundraising for charity; this must be signed off by senior management before any emails are sent.

Using, uploading or downloading any commercial software or any software not approved by ICT is not acceptable. This includes using third-party browsers or VPNs to bypass internet filtering and monitoring.

You must not try to bypass, uninstall or compromises antivirus, antimalware and anti-spyware software, and don't open any files from removable media, or from the internet, without first checking that they are free from virus or malware.

9. What might we monitor?

In order to keep the network secure and available for all, and to help protect everyone in our learning community, we will monitor certain aspects of ICT and network use. This may include looking at the volume of internet, email and network traffic, logging any internet sites visited, and logging keywords that are rejected by our Firewall.

Our school MIS package, used by staff to record information about learners and the day-to-day business of the school, has an audit function. We will use this periodically to monitor access to the system, and to ensure that it is only being used for operational reasons that enhance teaching and learning.

The specific content of any transactions will only be monitored if there is a suspicion of improper use. If there are concerns about the way a student or learner is using the ICT facilities, this may lead to further conversations with teachers or senior managers.

ICT staff are permitted to directly access staff [and learner's] email accounts if authorised by senior management, to check that they are being used appropriately. You will be told if that has occurred.

10. What could happen if you don't follow these rules

These rules are intended to keep everyone in our learning community safe, and to ensure that we all benefit from the opportunities for improved and enjoyable teaching and learning that ICT can offer.

Anyone failing to comply with these guidelines can expect further action to be taken. For staff this could include disciplinary action under the disciplinary procedure.

If any criminal acts have taken place, then we will involve the Police as appropriate. They will have full access to all logs, back-ups and records that we hold in relation to any alleged wrong-doing.

Appendix 1

Norton Canes High School
Acceptable User Agreement (AUA) – Staff & Volunteers

School Policy

New technologies have become integral to the lives of children and young people today, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should always have an entitlement to safe access to the internet and digital technologies.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, RDS etc.) out of school, and to the exceptional need for transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use

my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner and through a school email address.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school's ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will 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 download or distribute copies (including music and videos).

Norton Canes High School
Acceptable User Agreement (AUA) – Staff & Volunteers

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

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: .....

Signed: .....

Date: .....

This form will be kept by the Data Protection administrator for a period of no longer than six years after leaving employment and will be securely shredded.

Norton Canes High School
Acceptable User Agreement (AUA) – Pupils

School policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *learners* to agree to be responsible users.

Acceptable Use Agreement

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

For my own personal safety:

- I understand that the schools will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

- I understand that the school's systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school's systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of 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 strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

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 own personal devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if I can use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me 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 hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites while on the school network.

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 (including music and videos)
- 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 the school also has the right to act 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 online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page 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 systems and devices.

Norton Canes High School
Acceptable User Agreement (AUA) – Pupils

Learner Acceptable Use Agreement Form

This form relates to the learner acceptable use agreement; to which it is attached.

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 systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school's systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, RDS, website etc.

Name of Learner: .....

Group/Class: .....

Signed: .....

Date: .....

Norton Canes High School
Acceptable User Agreement (AUA) – Community Users

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, whatever the cause.
- I will 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 download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices

I have read and understand the above and agree to use the school systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Norton Canes High School
Wireless User Agreement (AUA) – Staff & Volunteers

This acceptable use policy (AUP) is subject to change at any time without notice. Any such changes will be those considered by the School in its reasonable opinion to be necessary for the smooth and safe running of the wireless service and the School.

1. Introduction
The wireless service is provided by Norton Canes High School which provides wireless access around areas of the school. The wireless network is available to any member of the NCHS staff with a computer username and password. The wireless network is provided exclusively for staff and network keys should not be shared or made available to students without the prior agreement of the Network Manager and only upon the completion of an appropriate AUP.

2. Fees & charges for the wireless service

There are no charges for connecting to or using the wireless service. Users would normally supply their own wireless computer device.

3. Technical Information
The wireless network supports 802.11a/b/g/n connections and the only protocol supported is TCP/IP via DHCP. Users must ensure that their equipment matches this configuration. The School does not guarantee connectivity with all manufacturers' equipment.

4. Service support
The School provides very limited technical support to users connecting to the wireless service.

The School does not guarantee that the wireless service will be fault free and at times it may not be possible to inform user of any disruption to or suspension of the service. Any breakdown in service will be rectified as soon as possible, but during holidays and over a weekend this may not always be the next working day.

5. Terms & conditions
The wireless service must be used in accordance with the School's Computer Use Agreement, the Computer Misuse Act (1990) and the law.

All wireless service users must adhere to copyright and license laws. The Wireless must not be used for any illegal or inappropriate activity.

I agree to the terms and conditions of the wireless AUP.

Staff/Volunteer Name: .....

Signed: .....

Date: .....

This form will be kept by the Data Protection administrator for a period of no longer than six years after leaving employment and will be securely shredded.

Advisory Code of Practice in the use of Social Networking Sites and Electronic Media

1. Protecting Yourself and Others in the Use of Social Networking Sites and

Electronic Media.

This code of practice provides staff with guidance to ensure that they are taking the necessary steps to protect themselves and others against online bullying. It also provides staff with practical guidance on how they can ensure that their conduct in relation to social networking sites and electronic media is in accordance with the code of conduct for all Local Government staff as interpreted by Staffordshire County School in relation to social networking sites and electronic media.

2. Online Bullying

Definition: “Online bullying is the use of Information and Communications Technology (ICT), particularly mobile phones and internet, deliberately to upset someone else”

Norton Canes High School supports the view that online bullying represents a cruel, dangerous and inescapable form of bullying that causes humiliation, stress and trauma to its victims, and so is committed to the view that online bullying is not acceptable and will not be tolerated.

3. Legislation

Although bullying is not a specific criminal offence, criminal law exists to prevent certain behaviours. These behaviours may constitute harassment, or cause a fear of violence. Sending indecent, grossly offensive or threatening letters, electronic communications or other articles to another person is illegal.

Other legislation protects against the publication of obscene articles or data (e.g. over a school intranet), hacking into someone else’s computer, invading their privacy, damaging their reputation or engaging in anti-social acts.

4. Protecting yourself against Online Bullying

There are simple measures that you can take to safeguard against online bullying:

- being careful about personal information and images posted on the internet;
- not leaving your mobile phone or personal computer around for others to gain access or leaving details on view when left unattended;
- choosing hard-to-guess passwords and not letting anyone else know them;
- being aware of the risks of giving your mobile number or personal e-mail address to others;
- making use of blocking facilities made available by website and service providers;
- not replying or retaliating to a bullying message;
- saving evidence of offending messages;
- making sure you inform others of any mobile phone or online bullying or harassment in accordance with relevant policies.

5. What action you can take

You can report any incidents in relation to Online bullying in the work environment in accordance with county School's Harassment and Bullying policy. If you make a complaint you have a right to have it investigated, and to seek assistance from managers, colleagues or trade unions in so doing.

Online bullying complaints will be investigated to obtain any evidence available and you can support this process by:

- logging any incidents;
- noting the dates, times and content of messages and, where possible, the sender's identity or web address.

Taking an accurate copy of the whole web page address, for example, helps service providers to locate offending material. Such evidence may be required also to show to those who need to know, including police. Saving evidence of texts and images on the device itself is useful. It is important they are not deleted.

In the non-work environment it may be appropriate to report incidents of Online bullying direct to an internet service provider or mobile phone company. Content may be blocked and / or removed if it is illegal or breaks the provider's own terms and conditions. Some providers issue conduct warnings to users and are able to delete the accounts of those who have broken the rules.

Some cases may raise allegations against staff and in such cases, immediate referral should be made via the First Response Team to one of the Local Authority Designated Officers (LADO) who will provide initial advice and guidance.

6. Code of Conduct

As a Condition of Service, all staff are expected to maintain conduct of the highest standard such that public confidence in their integrity is maintained. This employment obligation is also reinforced, in relation to certain posts, by a duty to comply with other external standards – as applies, for example, to Social Workers under the GNCHS Codes of Conduct, or the requirements of professional bodies such as the Law Society.

You are reminded that care should be taken with the personal use of Social Networking Sites to ensure that the integrity of the county School is maintained and to this end you should ensure that you take account of the expectations of all staff with regard to all aspects of the staff code of conduct when posting information, messages, pictures or video footage these may include:

- Bringing the County School/ Norton Canes High School and its members into disrepute
- Confidentiality
- Political restrictions

Care should also be taken of the legislative measures that already exist e.g. Invasion of privacy, harassment,

7. Safeguarding

In order to safeguard yourself and potentially vulnerable adults and young people who you may work with you should ensure that your behaviour with regard to social networking sites is consistent with the standards of behaviour expected in normal day to day interactions with vulnerable adults and young people.

Communication that is undertaken via social networking sites is comparable to 'one to one' interaction in other contexts, and individuals should avoid any activity which would lead any reasonable person to question their motivation and intentions.

You are reminded that it is expected that you:

- Always act in such a way as to promote and safeguard the well-being and interests of service users and colleagues.
- Take all reasonable steps to ensure that relationships with service users and colleagues are such that there can be no suggestion of impropriety whether by word or action.

c) Develop a friendly relationship between employee and service users, with clear boundaries. It is deemed an abuse of that professional relationship for an employee:

- to enter into an improper relationship with a service user;
- to show favour towards a particular service user;
- to act in a threatening or aggressive manner or to use foul, abusive or profane language;
- to endeavour to exert an undue influence with regard to personal attitudes, opinions or behaviour which is in no way connected to the work of the Service.

d) Take all reasonable steps to ensure that no action or omission on your part or within your sphere of influence is detrimental to the condition or safety of service users

In order to preserve these standards of behaviour it is recommended that you decline any request from an existing or previous service user to be a “friend” on your Social Network Site. It is inappropriate to request contact with an existing or previous user of the service via this medium or any other form of electronic medium.

It is acknowledged that you may accept a service user as a “friend” unintentionally and where this occurs you are advised to ensure that you remove this access as soon as you become aware of their status. You should do this in a way that does not jeopardise your professional relationship and should inform your Line Manager, if any significant conversation or activity occurs.

All staff are advised to ensure that when setting up social networking sites they should make full use of the range of tools which enable the access to personal information to be restricted.

8. Links to Policies

Harassment & Bullying at Work Policy

ICT Acceptable Use Agreement

Whistle Blowing Policy

Local code of Conduct for County School Staff

N.B. This code is for the guidance of staff. Any resulting consequences of disregarding this code, may lead to formal action being taken.

What is a Protective Marking Scheme?

A protective marking scheme is a way of assigning information to a security level which, in turn, relates to a range of pre-defined controls designed to ensure the information is handled properly.

All staff within the County School have been asked to securely mark their documents. This means that when you receive communications from them in future it will be labelled to conform to the scheme. It is not a requirement for Governors to conform to the scheme.

The security levels are:

Public	This is meant for documents/emails that would have no restriction at all and no level of security requirement. Very often the intention of creating such documents would be to publish them. Often informative by their nature. There is no need to mark public documents.
NCHS Use	Not for release to the public, i.e. information not approved for general release outside NCHS. This information, if lost, may not result in a financial loss or damage the image of the School but may lead to misunderstanding or misinterpretation of its content without a context and therefore should not be automatically released.
Restricted	Not for release to all staff, i.e. this will be information that should not be readily accessible to the public or to all staff. Release of this information may cause distress to individuals, affect operational matters, undermine the delivery of services. This information would require explicit authority to be shared outside its restrictions or removed from the Authority.
Confidential	Would cause serious damage if released, i.e. Highly sensitive internal documents which may cause serious damage to the School if released may place people or assets at risk. This information should be afforded the highest sensitivity and security and would require the explicit authority of a senior manager to be used outside the restriction that would be placed upon it.

As long as the mark is clearly visible it can appear anywhere. Where emails are concerned the mark should appear in the subject field. For other documents it can appear in the header or footer.

NORTON CANES HIGH SCHOOL
PHOTOGRAPHIC CONSENT

Use of Digital / Video Images

To comply with Data Protection law (including the General Data Protection Regulation and associated legislation), we are required to obtain your consent so that we may take and use photographs and video recordings of your child.

Photography and videography may be used at Norton Canes High School for the purposes set out below. Only images of children in suitable dress will be recorded and shared. Staff are not allowed to take photographs or videos on their personal equipment. In specific cases personal phones may be used to collect video evidence of curriculum activities. Where this is the case the student will record themselves on their own phone.

When sharing photographs with external third parties we will endeavour to:

- avoid providing the child's name where the child's image is shared;
- avoid providing the child's images where the child's name is shared;
- use only children's first names, rather than their full names (except in exceptional circumstances where we may provide the first initial of their surname to distinguish them).

When sharing video recordings with external third parties we will endeavour to:

- avoid providing the children's names within the video recording;
- avoid providing children's full names in crediting of video recordings.

If we would like your child's image linked to their name we would contact you separately for permission (for example, if your child won a competition and wanted to be named in press/literature).

Permission Form

We would like your consent to take photos and videos of your child and use them in the ways described below. If you are not happy for us to do this, we will accommodate your preferences.

Please tick the relevant box(es) below and return this form to school.

I am happy for photos/videos of my child to be used on the school website. ☐
I am happy for photos of my child to be used in the school prospectus. ☐
I am happy for photos/videos of my child to be used on school social media accounts ☐
I am happy for photos/videos of my child to be used on promotional materials (i.e. posters, banners, etc.) ☐
I give permission for my child's personal phone to be used to collect curriculum evidence ☐

You are free to withdraw your consent at any time. If you wish to withdraw your consent for any of the above activities, please contact the academy office. If you have any other questions, please get in touch.

Child's name	
Parent/Carer Signature	
Date	

Additional Guidelines for Educators Using Social Networking Sites

Social networks are rapidly growing in popularity and use by all ages in society. The most popular social networks are web-based, commercial, and not purposely designed for educational use. They include sites like Facebook, MySpace and Bebo. For individuals, social networking sites provide tremendous potential opportunities for staying in touch with friends and family.

Other educational networking sites are also growing in use. These sites are usually restricted to only certain users and not available to the general public. These include resources such as Moodle, educational wikis and professional online communities such as the SLN2.

As educators we have a professional image to uphold and how we conduct ourselves online helps determine this image. As reported by the media, there have been instances of educators demonstrating professional misconduct while engaging in inappropriate dialogue about their schools and/or students or posting pictures and videos of themselves engaged in inappropriate activity.

One of the hallmarks of social networks is the ability to "friend" others – creating a group of others that share interests and personal news. The Local Authority strongly discourages teachers from accepting invitations to friend students within these social networking sites (don't do it!). When students gain access into a teacher's network of friends and acquaintances and are able to view personal photos, the student-teacher dynamic is altered. Friending students provide more information than one should share in an educational setting. It is important to maintain a professional relationship with students to avoid relationships that could cause bias in the classroom.

For the protection of your professional reputation, the following is strongly recommended

Friends and friending

- Do not accept students as friends on personal social networking sites. Decline any student-initiated friend requests.
- Do not initiate friendships with students
- Remember that people classified as "friends" have the ability to download and share your information with others.
- If you wish to use networking protocols as a part of the educational process, please work with your administrators and technology staff to identify and use a restricted, school endorsed networking platforms.

Content

- Do not use commentary deemed to be defamatory, obscene, proprietary, or libelous. Exercise caution with regards to exaggeration, colorful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterizations.
- Weigh whether a particular posting puts your effectiveness as a teacher at risk.
- Post only what you want the world to see. Imagine your students, their parents, your administrator, visiting your site. It is not like posting something to your web site or blog and then realizing that a story or photo should be taken down. On a social networking site, basically once you post something it may be available, even after it is removed from the site.
- Do not discuss students or coworkers or publicly criticize school policies or personnel.
- Do not post images that include students.
- Security
- Due to security risks, be cautious when installing the external applications that work with the social networking site. Examples of these sites are calendar programs and games.

- Run updated malware protection to avoid infections of spyware and adware that social networking sites might place on your computer.
- Be careful not to fall for phishing scams that arrive via email or on your wall, providing a link for you to click, leading to a fake login page.
- Visit your profile's security and privacy settings. At a minimum, educators should have all privacy settings set to "only friends". "Friends of friends" and "Networks and Friends" open your content to a large group of unknown people. Your privacy and that of your family may be a risk. People you do not know may be looking at you, your home, your kids, your grandkids, - your lives!

Please stay informed and cautious in the use of all new networking technologies.

User agreement for the use of personal devices to record or photograph for curriculum or coursework evidence.

Videoing and photography in schools is subject to the Data Protection Act 1998 regarding the rights of individuals to have information of a personal nature treated in an appropriate manner and the Human Rights Act 1998, protecting the privacy of individuals and families. As well as these statutory rights, restrictions on video and photography arise from issues of Safeguarding and Copyright in performances. This is because an image of a child is personal data for the purpose of the Act, and it is a requirement that consent is obtained from the parent of a child or young person under the age of 18 years for any photographs or video recordings.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Therefore videos recorded in school must not be uploaded. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

Video and photography by School Staff and students

School staff and students can be involved in the video and photography of other students and staff for the purpose of curriculum or course work. Students should only video other students under the direction and supervision of the teacher.

At no point should students be instructed they must use personal devices for the purposes of collecting digital images. Students, under exceptional circumstances may be allowed to use their own devices although the school cannot be held responsible for damage and loss that may occur should they choose to do so.

School recording devices will always be available through prior agreement.

Staff are allowed to take digital / video images, using School equipment, to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Video must be for intended purpose only.

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Digital images collected for the purpose of curriculum or coursework must not be copied, shared, published or redistributed without the written permission of Norton Canes High School.

Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Video's or photographic images taken by staff or students whilst in school remain the property of Norton Canes High School.

Written permission from parents or carers will be obtained before photographs or videos of students are taken.

Cameras and mobile phones are prohibited in the toilet or changing areas of Norton Canes High School.

Digital images taken off site for the purpose of editing remain the property of Norton Canes High School and should be deleted from all devices as per the attached user agreement once the coursework has been submitted.

Staff should maintain a log of each occasion that personal devices have been used to record other students. This log should be available at any point for the purpose of accountability and safe guarding.

It is good practice for colleagues to confirm what will happen to video evidence used to assess practical elements of an examination with the external examiner during their visit to the school.

Pupils need to ensure that failure to comply could lead to disqualification

Consent form for School staff commissioning photography

To Name of parent or guardian:

Name of child:

School the child attends: **Norton Canes High School**

Location of digital image recording:

As part of their coursework students would like to *take photographs / *make a video recording of your *child / *children for the purpose of providing evidence. To comply with the Data Protection Act 1998, they need your permission before we take any images of your *child / *children.

Please sign and date the form where shown then return the completed form to:
Head teacher Norton Canes High School.

Parental Consent

I consent to digital images of my child being recorded for the purpose of providing evidence for curriculum or coursework.

I understand these images may be recorded on another students personal devices and where this is the case students will have signed a user agreement form and be bound by it.

Signed…… Parent / Guardian

Please print …….

Date ……

Pupil agreement

If using my personal device or a school device to record other students for the purpose of coursework I agree to abide by the policy outlined above.

Signed…… Parent / Guardian Please print
……..

Date ……

Norton Canes High School
Burntwood Road
Norton Cane
Cannock
WS11 9SP
T: 01543 62260
Email: office@nortoncanes-high.staffs.sch.uk