NORTON CANES HIGH SCHOOL
E-SAFETY POLICY

Formatted: Justified

1. Introduction

New technologies have become integral to the lives of young people in today's society, both within the school and beyond. The Internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can provide information, stimulate discussion, promote creativity and create awareness. They consequently make a major contribution to effective learning. Young people should have an entitlement to use ICT safely. This policy is designed to ensure that the day to day activities in school and beyond are E-safe. It incorporates the requirements of a wide range of legislation which is summarized in APPENDIX 1.

2. Links to Other Policies

This policy should be read in conjunction with the Security Policy, Freedom of Information, Code of Conduct for Staff, Code of Conduct for Students and the Safeguarding Policy.

3. Data Protection

Staff must ensure that they:

- Ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using secure password protected devices and / or encryption.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
- The data should be encrypted or password protected
- The device should be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- The device should offer approved virus and malware checking software
- The data must be securely deleted from the device once it has been transferred or its use is complete

4. Acceptable Use Agreements

The school will try to ensure that students, staff, parents and visitors will have good access to ICT to enhance learning and we will, in return, expect them to agree to be responsible users including:

- Staying safe while using the internet and other communications technologies for educational use with consideration to Content, Contact & Conduct.
- Ensuring that school ICT systems are protected from accidental or deliberate misuse that could put the security of the systems and users at risk. Signing and adhering to Acceptable Use Agreements (AUA) before accessing our ICT systems. (See APPENDICES 2-5 & 10)

[Appendix 3a is new] Wireless

5. Educating Students for Safe Use

The technological protection for students will be underpinned by an educational approach including:

- A planned E-safety programme within ICT and PHSE which will cover the use of ICT and new technologies both in and outside school.
- Key E-safety messages will be reinforced as part of the planned programme of assemblies and tutorial activities.
- Students will be taught in all lessons to be critically aware of the materials they access on-line and be guided to validate the accuracy of information.
- Students will be helped to understand the need for the student Acceptable Use Agreement.
- Students will be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- The rules for use of ICT systems and the internet will be posted in ICT rooms.
- Staff will act as good role models in their use of ICT, the internet and mobile devices.

6. Educating Parents / Carers and the Extended Family

Parents and carers play an essential role in the education of their children and in the monitoring and regulation of their children's on-line experiences. The school will seek to provide information and raise their awareness through:

- Letters, newsletters, the school web site and VLE.
- Parent evenings.
- Information distributed via students following E-safety modules.

7. Ensuring Best Practice in ICT to Enhance Teaching and Learning

E-safety should be a focus in all areas of the curriculum and staff should reinforce E-safety messages in the use of ICT across the curriculum including:

- When using the internet in lessons it is best practice for students to be guided to sites checked as suitable for their use and that the processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. Requests for website release should be made on an appropriate request pro-forma.

- Students should be taught in all lessons to be critically aware of the materials they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet and to be aware of the potential consequences of plagiarism, particularly with respect to examination coursework.

8. Internet Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. Staffordshire schools automatically receive a filtered broadband service through the broadband connectivity, with some flexibility for changes at school level. This service is intended to prevent users accessing material that would be regarded as illegal and / or inappropriate in an educational environment, as defined in the Filtering Policy. Because the content on the web changes dynamically and new technologies are constantly being developed, it is not possible for any filtering service to be 100% effective. Filtering is only one element in a larger strategy for E-safety and acceptable use.

Day to Day Responsibilities

The most senior ICT Technician and the Head of ICT will be jointly responsible for the day to day management of the school's filtering system. They will manage it in line with this policy and will keep records of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances, and to protect those responsible, changes to the school filtering service must:

- Be logged in change control logs
- Be reported to the Head of ICT prior to changes being made

All users have a responsibility to report immediately to the senior most ICT Technician or Head of ICT any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering and security systems in place to prevent access to such materials.

Awareness

Students will be made aware of the importance of filtering systems through the E-safety education programme covered in year 7 and this will be reinforced throughout ICT lessons in years 8 – 11. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- Signing and accepting the AUA
- Induction training
- Staff meetings, briefings and INSET.

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through E-safety awareness sessions, newsletters and the student planner.

9. Training

Staff will receive E-safety training to help them understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal E-safety training will be made available to staff (these will be recorded). It is expected that some staff will identify E-safety as a training need within the performance management process.
- All new staff will receive E-safety training as part of their induction programme, ensuring that they fully understand the school E-safety policy and Acceptable Use Policies
- The E-safety Coordinator will receive regular updates through attendance at LA / training sessions and by reviewing guidance documents released by LA and others.
- This E-safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-safety Coordinator will provide advice, guidance and training as required to individuals as required.

Governors will be offered E-safety training and awareness sessions, particularly those who are members involved in E-safety, health and safety or child protection. This may be joining staff during an INSET opportunity.

10. Roles and Responsibilities

The following section outlines the roles and responsibilities for E-safety of individuals and groups within Norton Canes High School.

Governors: are responsible for the approval of the E-safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Lettings and Premises Committee who will receive information about E-safety incidents and monitoring reports. A designated member of the Governing Body will have the role of E-safety Governor. The role of the E-safety Governor will include meetings with the E-safety Co-ordinator to monitor E-safety, filtering incident logs and control logs and reporting to relevant Governors meetings.

School Leaders: The Headteacher has overall responsibility for ensuring the safety (including E-safety) of members of the school community.

The day to day responsibility for E-safety will be delegated to the E-safety Co-ordinator (Head of ICT) who will work with the member of the Senior Management team responsible for safeguarding.

The Headteacher and Senior Leaders are responsible for ensuring that the E-safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their E-safety roles and to train other colleagues, as relevant

The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. The member of the Senior Management team responsible for safeguarding will work in conjunction with the E-safety officer and if necessary the Staffordshire Safeguarding Children's Board (SSCB) in this process.

The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the E-safety Co-ordinator / Officer.
The Headteacher and the Senior Management Team member responsible for safeguarding should be aware of the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff.

Child Protection Officer along with the Head of ICT: Will have the day to day responsibility for E-safety issues. Their roles will include:

- Leading issues of E-safety through the E-safety committee.
- Taking day to day responsibility for E-safety issues and having a leading role in establishing and reviewing the school E-safety policies / documents
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place.
- Providing training and advice for staff
- Liaising with the Local Authority
- Liaising with school ICT technical staff
- Receiving reports of E-safety incidents and creates a log of incidents to inform future E-safety developments
- Meeting with E-safety Governor to discuss current issues, review incident logs and filtering / change control logs
- Attending relevant meeting / committee of Governors
- Reporting to Senior Leadership Team

The Most Senior ICT Technician: Is responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- That the school meets the E-safety technical requirements outlined in the Staffordshire Security Policy and Acceptable Usage Policy and any relevant Local Authority E-safety Policy and guidance
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- Staffordshire Learning Network provide schools with the RM solution 'Safety Net Plus'. The software is categorised into nine sections i.e. pornography, SMS messaging etc., by default several sections and websites are filtered and access is denied.
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single individual.

- The E-safety Co-ordinator keeps up to date with E-safety technical information in order to effectively carry out the E-safety role and to inform and update others as relevant
- That the use of the network, Virtual Learning Environment (VLE), remote access and email are regularly monitored in order that any misuse or attempted misuse can be reported to the E-safety Co-ordinator for investigation, action and sanction where appropriate.
- That Securas monitoring software / systems are implemented and updated as agreed.

Teaching and Support Staff: are responsible for ensuring that:

They have an up to date awareness of E-safety matters and of the current school E-safety policy and practices and are familiar with the Staffordshire County Council Code of Practice for Social Networking and E-Media found in APPENDIX 6
They have read, understood and signed the school Staff Acceptable Use Agreement (APPENDIX 3) and (APPENDIX 3a)

- They report any suspected misuse or problem to the appropriate person for investigation, action and sanction where appropriate.
- Digital communications with students (email, Virtual Learning Environment (VLE),voice) should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Students understand and follow the school E-safety and acceptable use policy
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of E-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- They apply the guidelines set out in the “Protective Marking Policy” (Appendix 7) where appropriate.

The CPD Coordinator: Should ensure that the Child protection Officer and other relevant staff have, where possible, access to appropriate training on E-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal or inappropriate materials
- Inappropriate on-line contact with adults and other strangers
- Potential or actual incidents of grooming
- Cyber-bullying

The member of the Senior Management team responsible for safeguarding **and** the delegated Governor , The senior ICT technician will assist the E-safety Coordinator with:

- The production, review and monitoring of the school E-safety policy and related documents.
- The production review and monitoring of the school filtering process

,

E-safety should be raised as an issue with the school council and their views forwarded via the SLT member.

Students:

- Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy (APPENDIX 2), which they will be expected to sign before being given access to school systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good E-safety practice when using digital technologies out of school and realise that the school's E-safety Policy covers their actions out of school, if related to their membership of the school
- Parents and Carers: play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the website and VLE. Parents and carers will be responsible for:
- Accessing the school website, VLE and on-line student records in accordance with the relevant school Acceptable Use Policy.
- Signing the Parent and Carer Acceptable Use Agreement Form (APPENDIX 5) when collecting their access details to the school VLE. This also has details of the Student Use Agreement which the Parent/Carer will be asked to endorse through that signature.

Community Users and visitors who access school ICT systems, website or VLE: will be expected to accept or sign a Visitor Acceptable Use Agreement (APPENDIX 4), before being provided with access to school systems.

Approved by Governors: ……. Review Date:

APPENDIX 1

Legislative Background

This Policy is consistent with and complies with the following:

Computer Misuse Act 1990
This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

Establish the facts;

- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly

- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

APPENDIX 2

STUDENT ICT ACCEPTABLE USE AGREEMENT

In making this agreement I understand that:

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

- The school also has the right to take action 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).
- If I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, isolation, contact with parents and in the event of illegal activities involvement of the police and the possibility of exclusion
- 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.
- The school will monitor my use of the ICT systems, email and other digital communications.
- 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.

For my own personal safety I will:

- Not share my username and password, nor will I try to use any other person's username and password.
- Be aware of "stranger danger", when I am communicating on-line.
- Not disclose or share personal information about myself or others when on-line.
- Only meet people off-line that I have communicated with on-line when I have permission from a parent/carer and then only in a public place accompanied by an adult
- Immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable, when I see it on-line

For the safety and well-being of others 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.
- 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.
- Not take or distribute images of anyone without their permission.
- I will use the school system for educational purposes and in a responsible manner including:
- I 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 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 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.
- I will not attempt to use chat and social networking sites other than those within the SLN2 I will not try (unless I have permission) to make 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 ICT systems 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 only use my personal hand held / external devices (mobile phones / USB devices etc.) in school if I have permission. I understand that if given permission and if I do 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.
- 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.

✂……

STUDENT ICT ACCEPTABLE USE AGREEMENT

This form relates to the student Acceptable Use Agreement (AUA).
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.

- I have read and understand the Student ICT AUA and agree to follow these guidelines when:
- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) e.g. mobile phones, PDAs, cameras etc.
- I use my own equipment out of 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, VLE, website etc.

Name of Student …….. Tutor Group

Signature of Student …… Date

APPENDIX 3

STAFF ICT ACCEPTABLE USE AGREEMENT

(Includes Trainees, Visitors and others working in the school that access the ICT systems)

- In signing I accept the conditions set out below and agree to abide by the school's E-safety policy and staff Code of Conduct.
- I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner and that the ICT and related systems are school property.
- I will ensure that my information systems * use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school E-safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with students are compatible with my professional role.
- I will promote E-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I will adopt the guidelines set out in the protective marking policy (Appendix 7) as appropriate.
- I will avoid the use of personal recording equipment when working with students.
- The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

* Information systems includes telephone, fax etc.

Name: ……

Signed: …… Date: …….....

APPENDIX 3a

Norton Canes High School Wireless AUP

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 and will not share the access key.

Name _____ Username

Signed _____ Date

APPENDIX 4

VISITORS ICT ACCEPTABLE USE AGREEMENT

In signing I accept the conditions set out below and agree to abide by the school's E-safety policy.

- I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner and that the ICT and related systems are school property.
- I will ensure that my information systems * use is restricted to that necessary to achieve the agreed purpose of my visit.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding inappropriate use to the headteacher.
- The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

* Information systems includes telephone, fax etc.

Name: ……

Signed: …… Date: …….....

APPENDIX 5

PARENTS AND CARER ICT ACCEPTABLE USE AGREEMENT

In signing I accept the conditions set out below and agree to abide by the school's E-safety policy.

- I have received my personal logon information to the SLN2 Learning Platform.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager
- I understand that the school VLE, website, administration and related systems are school property.
- I will ensure that my use is restricted to that necessary to support my child.
- I understand that the school may monitor my use of its information systems* to ensure policy compliance.
- I will report any incidents of concern regarding inappropriate use to the headteacher.
- I am aware of the school's Acceptable Use Agreement for Students and endorse the signature of my child.
- The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

*Information systems includes telephone, fax etc.

Name: ……

Signed: …… Date: …….....

APPENDIX 6

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 employees with guidance to ensure that they are taking the necessary steps to protect themselves and others against cyber bullying. It also provides employees 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 employees as interpreted by Staffordshire County Council in relation to social networking sites and electronic media.

2. Cyber Bullying
Definition: "Cyber bullying is the use of Information and Communications Technology (ICT), particularly mobile phones and internet, deliberately to upset someone else"
[Cyber bullying: Guidance issued by the DCSF 2007]

Staffordshire County Council supports the view that cyber 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 cyber 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 Cyber Bullying
There are simple measures that you can take to safeguard against cyber 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 cyber bullying in the work environment in accordance with county council'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.

Cyber 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 cyber 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 employees 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 GSCC 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 council is maintained and to this end you should ensure that you take account of the expectations of all employees with regard to all aspects of the employees code of conduct when posting information, messages, pictures or video footage these may include:

- Bringing the County Council/ 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 employees 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. Other Policies
Harassment & Bullying at Work Policy
ICT Acceptable Use Agreement
Whistle Blowing Policy
Local code of Conduct for County Council Employees

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

APPENDIX 7

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 Council 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.
SCC Use	Not for release to the public, i.e. information not approved for general release outside SCC. This information, if lost, may not result in a financial loss or damage the image of the Council 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 council 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.

Formatted: Justified

Formatted: Justified

Formatted: Justified

Formatted: Justified

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.

APPENDIX 8

The use of Digital/Video Images – Parental Permission

Why do we use images?

Digital/video images play an important part in school life. They are used to support teaching and learning and to promote the school. They also serve as a record of music, drama, cultural and learning activities. Below is a summary of the kind of activities which students and staff are likely to take and display images of, although this list is not exhaustive:

Teaching and learning activities in lessons and out of school
School music and drama events
Sporting events
School visits and other activities such as the prom

Where will they be displayed?

They may appear on notice boards within school, in newsletters, occasionally on the school website and the public media.

Can parents record images?

The school allows images to be recorded by parents at school productions and events and you should be aware of this before allowing your child to take part. Images recorded by parents should:

Not be used for profit or gain
Never be used with the intention of causing embarrassment to any person in the image
Be used to celebrate the achievement of one or more individuals
Comply with acceptable standards of decency and good taste

The school complies with the Data Protection Act. We will avoid using a student's full name alongside photographs.

Parents are requested to sign the permission slip below to allow the school to take and use images of their children.

✂.....

Parental Permission Form – Use of Digital/Video Images

Name of Student _____ Tutor Group

As the parent/carer of the above student, I agree/do not agree (delete as appropriate) to the school taking and using digital/video images of my child/children.

I understand that the images will only be used in lines with the Code of Practice I have received or in publicity that reasonably celebrates achievement and promotes the work of the school.

I agree that if I take images of school events which include children other than my own I will abide by the above guidelines.

Name _____

Signed _____

Date_____ (Person with parental responsibility)

APPENDIX 9

The use of Digital/Video Images – Code of Practice

This Code of Practice specifies the manner in which Norton Canes High School will use and make available photographic images of pupils.

The school will:

Not use photographs in any form of internal or external publication where we do not have consent or where there is a written objection from a parent/guardian.

Allow parents to record images of school events and parents should be aware of this before allowing their child to participate. Where a parent wishes to make digital images at a school event they will be requested to register with the school.

Not use photographs/video of pupils in PE clothes or dancewear other than for instructional purposes where images are needed to demonstrate the activity to pupils or for use in promotional material unless specific permission is given.

Not reveal within the image personal details, such as date of birth, home address or telephone number.

In using materials of school age children for its purposes Norton Canes High School will:

Always ensure that parental permission has been given via this standard form.

Not to use images of children to illustrate child protection issues, fostering and adoption services or Youth offending Services.

APPENDIX 10

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.