Guilsborough Academy
Guilsborough Multi Academy Trust

Acceptable Use Policy

Guilsborough Multi Academy Trust

Policy Name	Acceptable Use
Committee	Environment and Health and Safety
Owner	Facilities Manager
Statutory	No

Date Ratified	Review Due
July 2022	July 2023

1. Introduction

The use of the Internet as a tool to develop learning and understanding is an integral part of Academy and home life. There are risks to using any form of communication which lies within the public domain therefore it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children use these technologies.

It is important that adults are clear about the procedures, for example, only contacting children and young people about homework via an academy email address, not a personal one, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

The Acceptable Use Policy sets out the policies, roles, responsibilities and procedures for the acceptable, safe and responsible use of online and communication technologies to safeguard adults and young people within the academy setting. It details how the academy will provide support and guidance to parents/carers for the safe and responsible use of these technologies. It sets out procedures for any unacceptable or misuse of these technologies by adults or young people.

2. Aims

- To set out policies for the effective use of online and communication technologies within teaching and the management of the academy.
- To safeguard young people within the academy setting by detailing appropriate and acceptable use of on-line and communication technologies.
- To ensure adults are clear about their responsibilities in the use of online and communication technologies both within and beyond the academy setting.
- To develop links with parents/carers ensuring input into policies and procedures with continued awareness of benefits and potential issues of on-line and communication technologies.
- To set out procedures for consultation with students on these issues
- To set out current practice to achieve these aims and the procedures for their review.
- To outline the roles and responsibilities for policy and implementation.

3. Protection of students from unsuitable content.

These risks include:

- Commercial issues with spam and other inappropriate e-mail.
- Grooming by predators, usually pretending to be someone younger than their true age.
- Illegal activities of downloading or copying any copyright materials and file-sharing via the Internet or any mobile device.
- Viruses.
- Cyber-bullying.
- Online content, which is abusive, racist or pornographic.

The academy will endeavour to ensure that students are aware of the risks of online contact. Measures will be taken to limit access to inappropriate sites and to detect and deter inappropriate and unwanted electronic contact between students.

Within the ICT schemes of work issues of Internet safety are raised and discussed (Appendix 1). This is supported within the life skills programme and ensure that the key safety messages are the same whether children and young people are on or offline engaging with other people. Cyber bullying is included within the Anti-Bullying Policy – latest version is available on the VLE.

Acceptable Use Rules and the letter for children and young people and parents/carers are outlined Appendix 2 and 3 and detail how students are expected to use the Internet and other technologies within academy, which includes downloading or printing of any materials. The rules are there for children and young people to understand what is expected of their behaviour and attitude when using the Internet which then enables them to take responsibility for their own actions.

No technical solution can prevent a determined individual from breaching the measures the academy puts in place to maximise student protection and the primary responsibility for ensuring correct use lies with the teacher. The academy will regularly assess with governors the appropriate technical response considering developments in technologies and the level of abuses reported. The current policy is detailed in Appendix 4.

All staff have a responsibility to report any breaches of the policy or inappropriate use of emails using the specified form (Appendix 5) and these will be investigated by the network manager. In particularly serious or sensitive cases this will be done in consultation with the e-safety leader and/or pastoral manager. The responsibilities of staff for their conduct and for that of students is detailed in Appendix 6.

All breaches of policy are logged, and patterns monitored. If there is a serious breach it should be reported to the governors.

4. Network security and reliability

An Anti-virus solution (Sophos, Impero and Smoothwall) is used to monitor and protect all network computers controlled by the academy and is updated on a regular basis. A firewall limits access to our network from unauthorised users. The network is also divided into separate subnets to limit access to services and information. At the last review, the network is divided into 10 virtual networks separating domain joined controlled Windows devices, Controlled Apple devices, student personal devices, staff personal devices and guest personal devices. Wherever possible client isolation is enabled to limit traffic between devices on our Wireless network. A filtering system is maintained which minimises the risk of deliberate or accidental access to inappropriate material. This is detailed in Appendix 4.

5. Use of own-devices and mobile phones in an 11-18 academy

Students are allowed to bring laptops and tablets into the academy as part of the BYOD scheme. There are many contexts when mobile devices and mobile phones and recording devices can be used positively within the classroom and to support learning. As the power of the devices continues to grow the range of such applications will increase.

We recognise that, within our rural catchment area, there are occasions, particularly when travelling to and from school, when contact with home during the day is necessary and the personal mobile phone can be the best way to do this.

The academy accepts that own-devices and mobile phones can be brought into the academy with the following provisos.

- Use of the device on site follows the academy's own rules.
- There is an absolute ban on the possession of mobile phones and other devices in public exams. This includes the controlled assessment coursework sessions.
- The use of mobile phones to bully, threaten or participate in sexual harassment/violence is forbidden and will be dealt with in the context of the academy's anti-bullying policy and sanctions.
- Pictures, recordings or videos of staff or students should not be taken without the consent of the person involved.
- Responsibility for the security and care of the device is solely that of the student.
- The academy reserves the right to confiscate and secure any device which is used outside these guidelines.

6. Responsibilities

Governors and Principal/Head of School

- It is the overall responsibility of the Principal/Head of School with the Governors to ensure that the academy has a comprehensive set of e-Safety policies which are reviewed, as necessary.
- Ensure that e-Safety aspects of Child Protection are addressed within the academy.

E-safety Governor

- Be aware of the academy's acceptable use policies and their implementation.
- challenge the academy about having appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT.

E-Safety Leader

- Implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed in order to establish a safe ICT learning environment.
- Promote e-Safety across the academy and curriculum within the framework of the academy development plan.
- Inform the Governors at the Health and Safety meetings about the implementation of the Acceptable Use policy, of or any updates to the e-Safety curriculum and ensure Governors know how this relates to child protection. Recorded breaches of the Acceptable Use policy will be reported to e-Safety leader, staff Health and Safety committee and annually to the Full Governor meetings
- Ensure that the AUP is reviewed annually, with up-to-date information available for all staff to teach e-Safety and for parents to feel informed and know where to go for advice.
- Report issues and update the Principal/Head of School and governors on a regular basis.
- Liaise with the Life skills, Child Protection and ICT leads and the network administrator so that policies and procedures are up to date to take account of any emerging issues and technologies.

Network Administrator

- Ensure there is appropriate and up to date anti-virus software and anti-spyware on the network PCs and laptops and that this is reviewed and updated on a regular basis.
- Ensure that the network functions on a continuous basis and that security policies are in place and implemented.
- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures and appropriate action is taken.

Appendix 1

E-safety in the Curriculum

Aim

To ensure that students at Guilsborough are protected and supported in their use of online technologies so that they know how to use them in a safe and responsible manner so that they can be in control and know what to do in the event of an incident.

We teach our children and young people how to use the Internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding and communicating effectively to further learning, through ICT and/or PSHE lessons where the following concepts, skills and competencies have been taught by the time they leave Year 11:

- Internet literacy
- making good judgements about websites and e-mails received
- knowledge of risks such as viruses and opening mail from a stranger
- access to resources that outline how to be safe and responsible when using any online technologies.
- knowledge of copyright and plagiarism issues
- file-sharing and downloading illegal content.
- uploading information – know what is safe to upload and not upload personal information.
- where to go for advice and how to report abuse

Students in Key Stage 3 learn the basics of e-safety as part of the schemes of work in years 7 and 8. They understand the risks associated with communicating digitally and understand the need for security of personal information.

Units of work focus on the issues of online communication, safe disclosure of personal information and the potential dangers of email, social networking and online chat rooms, cyber-bullying and acceptable use of IT facilities at academy and home. They are also introduced to standard ways of working and encouraged to follow good practice throughout their whole of their IT experience.

The tools available for use for students include:

- Internet access
- Email
- Video conferencing
- Weblogs (on-line diaries)
- Wikis (on-line encyclopaedia or dictionary)
- Instant Messaging
- An on-line personal space for adapting as a user to:
    - upload work
    - access calendars and diaries
    - blog

The personal space contains some information about the user. This area should be used as an opportunity to discuss with children and young people appropriate information to enter to ANY website asking for personal details (e.g., a social networking site) and should reflect key messages for any on-line use.

The personal space should not have personal photographs uploaded that reveal more than a general location, an activity (without close-ups of students' faces) or piece of work, without the express permission of parents/carers and academy. The sharing of photographs via weblogs, forums or any other means online should only occur after permission has been given by a parent/carer or member of staff.

Staff need to consider the risks and consequences of anything they or students post to a web or social networking sites, as inappropriate comments or images can reflect poorly on an individual and can affect future careers. Any outside communications need to be checked before they are sent.

It is our policy to ensure that we educate students in understanding the use of a public domain and the consequences of misusing it including the legal implications and law enforcement through relevant curriculum links.

Network security will ensure that students can only access the internet through their allocated login and password. Multiple login attempts, access of inappropriate sites and other breaches of policy will be monitored and investigated.

Appendix 2

Acceptable Use Rules for Students

The academy has provided ICT facilities for your use, offering access to a vast amount of information for use in studies and offering great potential to support your learning. The ICT facilities are provided and maintained for the benefit of the entire academy community, and
you are encouraged to use and enjoy these resources and help to ensure they remain available to all.

You are responsible for good behaviour with the resources and on the Internet just as you are in a classroom or an academy corridor.

Equipment

- Always get permission from the network manager before installing, attempting to install or storing programs of any type on the academy computers.
- All maintenance should be carried out by ICT support staff.
- Do not eat or drink in the vicinity of the ICT equipment.
- Turn off any equipment when you have finished using it unless you are instructed otherwise by a member of staff.

Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- If you find a computer that another user has forgotten to log off from then inform a member of staff.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings is unacceptable behaviour.
- Your files and communications may be monitored to ensure that you are using the system responsibly.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as antisocial on the Internet as it is on the street.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of staff. The sending of an email containing content likely to be unsuitable for children or academies is strictly forbidden.

Spam

- Be careful with your email address on the Internet.
- You may receive spam if you publish your email address on a Web site, in a posting to a news group or in an online form (eg to send an electronic greeting card).
- Never reply to a spam message, no matter how annoying! By replying, you let the sender know that your email address exists and then you are likely to receive more spam.
- Never unsubscribe using links in spam email. This lets the sender know your email address is active – you are likely to receive even more spam!
- Never open attachments! Files attached to spam email often contain viruses. Delete the email immediately.
- The account provided by the academy should be used for all communications with academy staff and for communicating with other students for academy work purposes.
- Webmail such as Hotmail should not be used at all in the academy. The exception to this is for Sixth form students to allow for UCAS and other transitional communication should they move into higher education.

- The use of email for bullying will be investigated and dealt with in accordance with the academy bullying policy.

Physical Security

- Students in an ICT room should be supervised by a member of academy staff at all times. You should not be sent around the academy to look for a vacant IT suite during lessons or to see if there are spare computers in an ICT suite when a lesson is taking place. You may be sent to an ICT room if a prior arrangement has been made with the teacher using that room by your teacher. The teacher in the ICT room will then be responsible for supervising you and you must follow their instructions. Alternatively, you may be sent to the LRC.
- Outside of lesson times (this includes "Before Academy", "Break Times", "Lunch Time" and "After Academy") no student should have any access without direct supervision from a member of staff (i.e. the supervisor is in the room all the time that students are there).
- Doors to ICT rooms should be kept locked at all times when vacant. Inform a member of staff if you know that an ICT room has been left open.

Images of students & staff

- You should always ask another student or a member of staff for permission before recording their image. If they do not give you permission, then you must respect their decision.
- Consider using group photos rather than photos of individual students.
- Any images of you held by the academy will be deleted once their period of use has expired, or you have left the academy.

Personal equipment

- Personal mobile phones and other portable devices such as portable digital assistants (PDAs) and MP3 players should be used according to academy rules.
- Use of personal mobile digital equipment for bullying will be investigated and dealt with in accordance with the academy bullying policy.
- Staff must not give out their personal mobile phone numbers to you.
- Staff may ask you for your mobile phone number during an academy trip or other event. You do not have to give it if you do not wish to. If you do give your mobile phone number to a member of staff, the record of your number will be destroyed after the trip or event.

Please read this document carefully. If you violate these provisions, you will be subject to disciplinary action. Where appropriate, the police may be involved.

Internet Acceptable Usage Rules for Student

The purpose of this policy is to ensure that users of the Academy network understand the way in which the Internet is to be used. The policy aims to ensure that the Internet is used effectively for its intended purpose, without infringing legal requirements or creating unnecessary risk. Users should read this policy alongside the ICT Acceptable Use Policy.

Guilsborough encourages users to make effective use of the Internet. Such use should always be lawful and appropriate. It should not compromise Guilsborough's information and computer systems nor have the potential to damage the academy's reputation.

Use of internet facilities

The academy expects all users to use the Internet responsibly and strictly according to the following conditions: For the purposes of this document, Internet usage means any connection to the Internet via Web browsing, external email or news groups.

Users shall not:

Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography (including child pornography)
- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting illegal acts
- any other information which may be offensive to other members of the academy community

If inappropriate material is accessed accidentally, you should immediately report this to your teacher so that this can be taken into account in monitoring.

Incidents which appear to involve deliberate access to Web sites, newsgroups and online groups that contain the following illegal material will be reported to the police:

- images of child abuse (images of children, apparently under 16 years old) involved in sexual activity or posed to be sexually provocative.
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist or homophobic material in the UK

If you accidentally access illegal material, you should immediately tell a teacher.

Users shall not:

- Use the academy facilities for running a private business
- Enter into any personal transaction that involves the academy in any way
- Visit sites that might be defamatory or incur liability on the part of the academy or adversely impact on the image of the Academy
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of the academy, or to the academy itself
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
    - financial information
    - personal information
    - databases and the information contained therein
    - computer/network access codes
    - business relationships

- Intentionally interfere with the normal operation of the Internet connection, including the spreading of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion such as playing network games) that substantially hinders others in their use of the Internet.

- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate.

Monitoring

The Academy will monitor and audit the use of the Internet to see whether users are complying with the policy. Any potential misuse identified will be reported to the Network Manager and/or other relevant person.

Appendix 3

e-Safety Rules

These e-Safety Rules help to protect students and the academy by describing acceptable and unacceptable computer use.

- The academy owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the academy.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The academy ICT systems may not be used for private purposes unless the Principal/Head of School has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The academy may exercise its right to monitor the use of the academy's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the academy's computer 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.

Guilsborough Academy

e-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Pupil:	***Form:***

Pupil's Agreement

- I have read and I understand the academy e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed:	***Date:***

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the academy rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access

I have read and understood the academy e-safety rules and give permission for my son / daughter to access the Internet. I understand that the academy will take all reasonable precautions to ensure that pupils cannot access inappropriate materials, but I appreciate that this is a difficult task.

I understand that the academy cannot be held responsible for the content of materials accessed through the Internet. I agree that the academy is not liable for any damages arising from use of the Internet facilities.

Signed:	***Date:***

Please print name:

Appendix 4

Technical Details

The standard level of filtering will be set to education environment appropriate content in order to allow teaching and support staff the freedom to research materials without the constraints of tight filtering. An additional system called Smoothwall is in place which allows flexibility of control ranging from monitoring only, used for staff at the academy to a “default deny” policy specifying allowed sites that can be used for students which are particularly vulnerable. In extreme cases or for short periods access can be completely disabled through this system as well.

The system includes a central database of known sites categorised as Obscene, pornographic, online shopping, gambling, gaming, educational, etc. Users can be grouped and allowed or disallowed access to the various categories. This database is regularly updated by the provider, based on automated reports from the client installs as well as research on their part. It is also augmented on a day to day basis locally by the network support team in response to feedback from teaching and support staff supervising the students. Additional categories and groups are also maintained locally to meet fluctuations in use. As a general structure students are grouped in years and allowed greater freedom to research in relation to the syllabus. Groups or individuals specifically requiring access can be allowed on agreement between department heads and the ICT co-ordinator. Logs of activity are kept for 3 months in order to allow retrospective investigation of violations of the AUP.

The log of breaches of policy will be discussed at regular meetings between the network manager and the e-safety leader and if they feel it necessary additional precautions and procedures will be agreed and documented within this document.

All staff and students have email accounts. Accounts will be accessed if there is evidence of unacceptable use. Automatically checking rejects emails containing particular words. This can be set at different levels for different user groups. There is a pastoral account to which students can send emails they find offensive.

Staff and students are to use their academy issued email addresses within academy and for any communication between home and academy only. A breach of this will be considered a misuse and will result in consequences. Parents/carers are encouraged to be involved with the monitoring of emails.

Teachers are expected to monitor their class use of emails and the Internet during lessons. Any incidents should be recorded on the Computer Misuse form.

The network manager is responsible for monitoring usage and maintaining the agreed filtering system. The network manager reports regularly to the e-Safety Leader.

Appendix 5

Breach of Acceptable Use Policy

Date: / /	Class:	
Period: AM 1 2 Break 3 4 Lunch PM 5		Approx time:
Student(s):		Member of staff:
Room:	Machine used:	
Nature of incident:		
Action Taken:		

Appendix 6

Use of ICT - Staff Protocols

1) Social Networks

Whilst Social Networks are mentioned later in this document it is felt that there is a need to clearly state the current stance of the academy.
There are numerous Social Network sites – to name but a few Facebook, Twitter, Google Plus, My Space, MSN, Chat, LinkedIn, Skype etc. If you are unsure if something is classed as a Social Network site please contact the Network Manager in writing.
No social network sites should be used to communicate with students.
This means adults should:

- Ensure that personal social networking sites are set at private and pupils are never listed as approved contacts
- Never use or access social networking sites of pupils

Although we can see the benefits to using them, without the correct protocols and protections in place these are open to too many opportunities for allegations to be made against staff.
In order to move this form of communication forward we are willing to support pilot projects in a controlled setting. If you wish to be part of a trial of this nature please put your proposal in writing to the Vice Principal/Head of School and the Network Manager explaining the educational benefits of your trial and the precautions you propose to take to ensure the safety of all involved.
Alternative forms of communication can be used to communicate with students through the academy's email system and via the VLE. These are both academy approved and monitored methods of communication.

2) **Communication with Pupils** (from the Guidance for Safer Working Practice for Adults Working with Children and Young People in Educational settings)

Communication between pupils and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.
Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to pupils including email, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. E-mail or text communications between an adult and a child young person outside agreed protocols may lead to disciplinary and/or criminal investigation. This also includes communications through internet based web sites.
Internal e-mail systems should only be used in accordance with the academy's policy.

3) Use of Internet Facilities

The academy expects all users to use the Internet responsibly and strictly according to the following conditions: For the purpose of this document, Internet usage means any connection to the Internet via Web browsing, external email or news groups.
Users shall not:

Visit internet sites, make, post, download, upload or pass on material, remarks, proposals or comments that contain or relate to:

- Pornography (including Child Pornography)
- Promoting discrimination of any kind
- Promoting racial or religious hatred
- Promoting illegal acts
- Any other information which may be offensive to other members of the academy community

If inappropriate material is accessed accidentally, you should immediately report this to your line manager.

Incidents that appear to involve deliberate access to Web sites, newsgroups and online groups that contain the following illegal material will be reported to the police:

- Images of child abuse, images of children involved in sexual activity or posed to be sexually provocative
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or homophobic material

If you accidentally access illegal material, you should immediately tell your line manager.

Users shall not:

- Use the academy facilities for running a private business
- Enter into any personal transaction that involves the academy in any way
- Visit sites that might be defamatory or incur liability on the part of the academy or adversely impact on the image of the academy
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of the academy, or to the academy itself
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
  - Financial information
  - Personal information
  - Databases and the information contained therein
  - Computer/network access codes
  - Business relationships
- Intentionally interfere with the normal operation of the internet connection, including the spreading of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion such as playing network games).
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate

4) **Data Protection** – Please see the academy's Data Protection Policy.

5) Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as antisocial on the Internet as it is on the street.

- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist or inappropriate content, always report such messages to your line manager.

6) Installing Software

- Only approved software should be installed onto laptops/netbooks. A list of approved programs is available on the academy's VLE. (See Appendix 7 for information on the academy laptop agreement.)
- Any required software not on the list should firstly be approved by the Network Manager in writing.

7) Equipment

- Always get permission from the network team before installing, attempting to install or storing programs of any type on the computers.
- All maintenance should be carried out by the ICT support staff
- Always check files brought in on removable media and only use them if they are found to be clean of viruses
- Do not eat or drink in the vicinity of the ICT equipment

8) Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else's logon name or password
- If you find a computer that another user has not logged off, log them out and inform their line manager
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings is unacceptable behaviour.
- Your files and communications may be monitored to ensure that you are using the system responsibly

9) IT Suite Security

- Students in an IT suite should be supervised by a member of academy staff at all times.
- Students should not be sent around the academy to look for a vacant IT suite during lessons or to see if there are spare computers in an IT suite when a lesson is taking place. A prior arrangement should be made with the teacher using the IT room and they will then take responsibility for this student.
- Doors to IT rooms should be kept locked at all times when vacant.

10) Monitoring

- The network team will inspect staff laptops/netbooks annually. Staff are responsible for submitting their machine for checking
- The use of the internet will be monitored to see whether users are complying with the academy's policy
- Email will be monitored through the office 365 platform.

Appendix 7

Guilsborough Academy Laptop Agreement

This form must be completed by all staff who are loaned a laptop which is owned by the academy.

- All teachers have been issued with a laptop. Where there is no network point in a classroom, the academy network should be accessible via the wireless link. The majority of the academy's communication is electronic and it is essential that staff log on every morning.
- All loaned laptops are for use solely in relation to academy business and should not be used for personal use.
- The security and safekeeping of an academy laptop when taken off the premises is the responsibility of the member of staff borrowing the machine. The academy insurance policy only covers for the theft of items when forced entry (e.g. into a property or car) can be proved. Therefore, laptops should not be left unattended and should be locked in the boot of a car.
- Laptops that are not the property of the academy and are used in the academy are not the responsibility of the academy. The ICT technical staff will not maintain these machines or install software.
- If a laptop is connected to the academy network, the academy is liable for all software installed on that machine; therefore, any laptop connected to the academy network must have valid software licences.
- Theft or damage to academy laptops should be reported immediately to Daniel Parker/Chris Williams.
- Staff should maintain cleanliness of their devices.
- Staff should be aware of the implications of the Data Protection Act before downloading information from SIMS onto laptops, especially in the event of the loss or left of a machine. Such information should only be kept on the laptop for as long as is necessary.
- All staff are asked to sign a statement covering the care and security of the laptop.

All staff must complete this section:

Full Name ………………………………………………………………………………

Home Address ………………………………………………………………………….

………………………………………………………Tel. No. ………………………

Supply staff must complete this section:

Name of Supply Agency …………………………………………………………….

Contact at Supply Agency …………………………..Tel. No. ……………………..

I understand that the loan of a laptop is solely for my use whilst I am employed on supply to work at Guilsborough Academy. When I leave, I must return the laptop to the Network Team before my final working day, or within 5 days of my last working day. Failure to do this will result in the supply agency being informed and the value of the laptop being deducted from my salary payment. This is likely to be in the region of £700.

Signed ………………………………………………… Date ………………………

Please print name ……………………………………………….

Conditions of the Loan - To be completed by all staff

I accept that it is my sole responsibility to care for the laptop assigned to me by the Academy. I agree:

- To keep it in a sound state of repair
- To only use the laptop in connection with your academy role and not for personal use.
- To report any problems or damage immediately to the Network Team. In the event of damage through negligence, I may be liable for the cost of repair
- Not to install any unlicensed software and I am accountable for any charges on me or the academy for having such software installed.
- To report any accidental access of inappropriate sites.
- To use the laptop only in accordance with academy policies. I understand that my use may be monitored and the machine examined if there is evidence of inappropriate use.
- To return the laptop to the Network Team promptly whenever asked to do so for any updated software or virus updates or other maintenance
- To return the laptop to the Network Team by the last working day of employment if I leave the Academy. Failure to do this may result in the value of the laptop being deducted from my final salary payment.
- To ensure the laptop is insured for theft or damage occurring out of academy
- Not to permit any person other than an employee of the Academy to use the laptop
- To keep to a minimum data which comes within the terms of the Data Protection Act, and to delete this from the laptop as soon as possible.
- To use the laptop within the terms of the academy's Acceptable Use Policy which is available in the policy area on the VLE

Details of Laptop Issued

Signed:……………………………………. ………

Print:…………………………………….... ………

Model:…………………………………………….

Serial Number:…………………………………….

Laptop Number:……………………………………

Date: ………………………………………………

Insurance guidance:

The laptop is covered by academy insurance at the academy. We are not covered for walk in theft. Laptops (and other portable valuables) should not be left visible and should be kept secure overnight.

The laptop is covered by academy insurance in transit but should not be left visible when the car is unoccupied.

It needs to be covered by home insurance at home. The value should be stated at £500 if it needs specifying.