Online Safety Statement of Practice

Date Drafted:	**November 2020**
Date Approved by Governors:	**03/12/2020**
Review Frequency:	**Annually**
To be Reviewed By:	**Mr S Patrick**

Online Safety Policy

This policy should be read in conjunction with the following policies:

- Behaviour Policy
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Anti-Discrimination Policy
- Staff IT Security Policy (see Appendix A)
- Student IT Code of Conduct and Parental consent for Internet access (see Appendix B and C)
- The Blended learning guidelines (which give advice around live lessons)

Aims and Scope

Safeguarding is a serious matter; at The Long Eaton School we use technology and the Internet across all areas of the curriculum. We are also mindful of how much our students use these technologies outside of school and we take seriously the need to educate them about using them safely. Online safeguarding, known as "Online Safety", is an area that is constantly evolving and as such, this policy will be reviewed on an annual basis or in response to any Online Safety policy issues as they arise, whichever is sooner.

The purpose of this policy is twofold:

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

This policy is available for anybody to read on our website. At the start of each year students and staff will be expected to sign the Students' Acceptable Use Policy and the Staff Acceptable Use Policy respectively. Parents will also be expected to counter-sign the student policy. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology, including the Internet.

Roles and Responsibilities

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any Online Safety incident to ensure that the policy is up to date and covers all aspects of technology use within the school;
- Ensure online-safety incidents are appropriately dealt with and that the policy was effective in managing those incidents;
- Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:
  - Keep up to date with emerging risks and threats through technology use.
  - Receive regular updates from the Headteacher with regards to training, identified risks and any incidents.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for Online Safety within the school. The day-to-day management of this will be delegated to a member of staff, the Online Safety Officer, as indicated below. The Headteacher will ensure that:

- Online Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, leadership team and governing body and parents.
- The designated Online Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All Online Safety incidents are dealt with promptly and appropriately.

Online Safety Officer
The day-to-day duties of the Online Safety Officer include:

- Keep up to date with the latest risks to children whilst using technology; familiarising themselves with the latest research and available resources for school and home use;
- Review this policy regularly and bring any matters to the attention of the Headteacher;
- Advising the Headteacher and governing body on all Online Safety matters;
- Advising on engaging parents and the wider school community on Online Safety matters at school and/or at home;
- Liaising with the local authority, IT technical support and other agencies as required.
- Responsibility for the Online Safety incident log; ensuring staff know what to report and ensure the appropriate audit trail.
- Ensuring any technical Online Safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support;
- Making themselves aware of any reporting function with technical Online Safety measures, i.e. internet filtering reporting function; and liaising with the Headteacher and responsible governor (see attached list of contacts) to decide on what may be appropriate for viewing.

All Staff
Staff are to ensure that:

- All details within this policy are understood. If anything is not understood, it should be brought to the attention of the Headteacher as soon as practically possible.
- Any Online Safety incident is reported to the Online Safety Officer (and an Online Safety Incident report is made), or in their absence, to the Headteacher. If uncertainty exists as to whether an incident involves Online Safety, staff should raise the issue with the Online Safety Officer or the Headteacher and defer to them.

All Students
The boundaries of use of ICT equipment and services in the school are given in the Student IT Code of Conduct, placed in prominent positions in each IT suite. Students are asked to sign acceptance of the IT Code of Conduct in the relevant place in their school-issued planner. Any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

Given the intensive use of IT within The Long Eaton School, Online Safety is embedded across our curriculum and students will be given the appropriate advice and guidance by staff. Messages about Online Safety will be reinforced in assembly and tutor activities. Similarly, all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers
Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, school newsletters and our website, the school will keep parents up to date with new and emerging Online Safety risks, and will involve parents in strategies to ensure that students are appropriately equipped.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such, parents are expected to give their permission for students to access and use the School's Internet and eMail facilities in the student's school-issued planner before any access can be granted to school ICT equipment or services (see Appendix B and C).

Technology

The Long Eaton School uses a range of devices, including PCs and laptops to support the day-to-day operation of the school and the education of all students. Students may also use their own mobile devices through the School's Bring Your Own Device (BYOD) network subject to express permission from the class teacher, appropriate observation and acceptance of the BYOD policy. In order to safeguard the student and in order to prevent loss of personal data, we employ the following technology or policies:

Computer Usage Monitoring /Classroom Management – We use Impero Software for the monitoring and logging of all activity by users in the school. It uses policies, word lists and website lists to detect and log (via screenshot, website/window history etc.) any student viewing unsuitable content, accessing indecent images, cyberbullying, grooming, identity theft, radicalisation and terrorism. Teaching staff have basic access to Impero for monitoring and interacting with students in their classroom. Any policy breaches by a student in their classroom is flagged up for the teacher via the Impero console. Teaching staff should pass on any screenshots/concerns they have about what a student has been up to/viewing to the IT Systems team who can then check the full logs/update the Internet filter etc.

Internet Filtering/Firewall – We use Sophos Unified Threat Management.
The Sophos Web Protection filter prevents malware infections, spyware and viruses from entering the network via the internet. It prevents access to inappropriate websites as determined by the age of the user and their role within school. (e.g. Yr7-9, Yr10-11, 6th Form and Staff all have different filtering levels based on what's appropriate to them). All website access is logged against each user across both the school network and any personal device connected to the BYOD network. All Internet filtering is reviewed in line with this policy or in response to an incident, whichever is sooner. The Online Safety Officer and IT Systems Team are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – We use Microsoft Office 365 for our e-mail solution along with its built in spam and anti-malware filters that prevents any infected email from being sent or received by users in the school.
Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data and spam email such as a "phishing" message intended to trick the recipient into handing over their personal data or login details for public (usually financial) websites.

Encryption and Data Protection – All school devices are configured to automatically store information – personal (as defined by the Data Protection Act 1998) or otherwise – on the central server, where it is secured and protected against theft or other loss in line with good practice. To protect information that may leave the school, all school devices are configured to encrypt removable storage media using the inbuilt Bitlocker functionality. While computer users have the option to *not* encrypt removable storage media (for instance, in a situation where it might not be appropriate i.e. data coming in), in such situations the removable media is automatically marked "read only" and cannot be written to until it has been encrypted. Any breach leading to loss or theft of device such as laptop or USB pen drives, is to be brought to the attention of the Headteacher and reported to the Police and Information Commissioners Office as appropriate.

Passwords – all staff and students need a unique username and password to access the computing facilities. The computer systems are configured to force users to choose "secure" passwords (a minimum of 8 characters featuring at least 3 of the following: uppercase letter, lowercase letter, number and an extended character) and to change the password every 90 days. Staff and student passwords will be changed if there is a compromise. The IT Systems Team are responsible for ensuring that passwords are changed when needed, though the ability to reset student passwords is delegated to key members of the teaching team to minimise disruption in lessons should a student be unable to access the computing facilities.

Anti-Virus and Windows Updates – All capable devices have anti-virus software installed and regularly install Windows Updates as managed by the IT Systems Team. The Network Manager will report to the Headteacher if there are any concerns.

The Long Eaton School accepts no liability for any loss or damage to students own mobile devices.

Safe Use

Internet, e-mail and software use in school.

Students must read and sign the Student Acceptable Use Policy at the beginning of each school year or after each major revision before they are allowed to use the Internet or e-mail at school. They must agree to the school viewing, with just reason and without notice, any emails they send or receive, material they store on the school's computers, or logs of websites they have visited.

School computer and Internet use must be appropriate to student educational activity. Students must only access those services they have been given permission to use and they must not access the internet or e-mail for inappropriate purposes. The work/activity on the Internet and e-mail must be directly related to the student's school work and they must not give their password or log-in name to anyone.

When working on a school PC or Laptop students must take care to "Lock" the laptop should they have reason to be away from their screen. This is to prevent other students from being able to access software and emails. If a student suspects that their account has been accessed by another student they should report this to a teacher immediately.

Students must not give personal information to anyone on the internet or by e-mail and they must not view, upload or download, or send by email, any material which may infringe copyright or is likely to be unsuitable for children or the school. This applies to any material of a violent, dangerous or racist nature or containing inappropriate sexual content. If they are unsure, they must ask a teacher for clarification.

Students must be polite and appreciate that other users might have different views than their own. The use of strong language, abusive language or aggressive behaviour is not allowed. Students must not write anything on a website or send by e-mail anything which could be offensive. They must not use the internet in or out of school to bully, threaten or abuse other students and they must not use the internet in or out of school for any purpose that may bring the school into disrepute.

In addition, when using e-mail, students should also be aware:

- E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers;
- Users are responsible for e-mail they send and for contacts made;
- Anonymous messages and chain letters are not permitted.

Staff Email Usage

All staff are reminded that emails are subject to Freedom of Information requests, and as such the school email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Social Networking and Online Bullying

The term 'social networking' refers to any website or digital resource designed to facilitate social interaction between people in either private or public online spaces.

Online bullying, e-bullying or cyber bullying, is defined as follows: 'the use of information and communication technologies such as email, [mobile] phone and text messages, instant messaging, defamatory personal websites and defamatory personal polling websites, to support deliberate, repeated, and hostile behaviour by an individual or a group, that is intended to harm others.'

If a student is being bullied online, he/she should immediately seek help from a teacher, parent or carer. They should not respond to the messages, but should keep a detailed diary recording information such as the content of the message, the date, the time, the caller ID, username, or email address, and whether the number was withheld

or not available. If space permits, the messages should also be stored on the phone, or in the email account, in case they are needed later as evidence.

Online bullying is considered as serious as any other form of bullying, and similar sanctions will be applied, as outlined in our Anti Bullying Policy.

Failure to comply with these rules will result in a ban, temporary or permanent, on the use of the Internet facilities at school and a letter informing their parents of the nature and breach of the rules. Appropriate sanctions and restrictions placed on access to school facilities may result and temporary or permanent exclusion for abuse of the school's ICT facilities and of the internet may be used in extreme or persistent cases.

Text Messaging/Mobile Phones

Students are advised to be careful about giving out their mobile phone number, and to tell those who have their number never to pass it on. The policy regarding the use of social media (above) applies equally to messages sent and received using mobile phones.

The sending of indecent images from one person to another though Digital Media Devices

Please refer to The Long Eaton School Safeguarding Policy for up to date guidance.

The use of ICT as part of our Blended Learning offer

Staff should refer to the guidance notes on Blending Learning for up to date information around this and should follow the procedures set out in that document.

THE LONG EATON SCHOOL

Staff ICT Security Policy

Rules, expectations and advice for users

The Long Eaton School

Staff IT security and usage policy

Introduction

Educational establishments are using computer facilities more and more to support their activities, and as a result school computer systems are containing increased amounts of sensitive and confidential data. IT resources are valuable and the confidentiality, integrity, availability and accurate processing of data are of considerable importance to the school and as such all users have a personal responsibility for IT security. This policy document contains rules and advice governing the safe and appropriate use of the School's network, e-mail and internet facilities and the storage of confidential information.

It applies to everyone that uses The Long Eaton School's ICT facilities either via school-provided or other equipment at home
(i.e Remote Desktop access from a personal PC or a staff laptop used as "stand alone") or in school itself.

As well as saying what E-mail and the Internet are allowed to be used for, the policy also provides guidance on the good practices that should be used and the practices that should be avoided.

Code of Conduct Declaration

All staff that have access to The Long Eaton School's computing facilities, including email and the internet connection, need to read this policy carefully and make sure that they understand it. The school will provide appropriate training where necessary. Staff then need to sign the declaration / consent form (enclosed at the back of this policy) to confirm that they have read, understood and will keep to the policy.

Staff must also understand that The Long Eaton School may take action against them in line with the disciplinary policy if they break the conditions of this policy – either wilfully or by act of neglect.

The school will keep the signed declaration in the relevant staff personnel file. Periodically, the school may ask staff to confirm that they still understand and accept the rules.

Staff must not use, or try to use the IT facilities of The Long Eaton School – including the email or Internet facilities - to create, distribute or display in any form, any activity that is or may be considered to be against the law, against school policies or that may lead to a legal claim being made against the school.

In this context, staff are not allowed to use the IT, email or Internet facilities for reasons that are:

- *pornographic or obscene;*
- *intimidating, discriminatory (for example; racist, sexist or homophobic) or that break our anti-harassment and equal opportunities policies in any other way;*
- *defamatory;*
- *hateful or encouraging violence or strong feelings;*
- *fraudulent or showing or encouraging criminal acts;*
- *unethical or may bring the school into disrepute; or*
- *a deliberate harmful attack on systems used, owned or otherwise run by the school.*

The school will only allow staff to access such material or do the above, with written confirmation, if it is necessary as part of an investigation or to ensure the safety of young people in the school's care.

Should staff inadvertently access such material, they must report the incident to the Network Manager immediately. If staff find or suspect anyone of using the computer system illegally or unethically, they must report it to the Network Manager who will advise the Headteacher or Chair of Governors.

Staff must not use the school IT, email or Internet facilities for inappropriate activities, such as chain letters, or for any other private activity that may be considered unreasonable during normal working hours.

The Long Eaton School

Staff IT security and usage policy

Specific conditions of the policy

Confidential or sensitive information

By using the school's ICT facilities, staff may become party to sensitive or confidential information relating to young or vulnerable people, or confidential information relating to the day-to-day business operations of the school.

Personally-identifiable or other personal information relating to students and other members of staff is governed under the Data Protection Act 1998 and staff must not break or by act or deed allow to be broken the conditions of this act under any circumstances. Such behaviour may also contravene the Computer Misuse Act 1990.

For advice about these conditions, staff should refer to the Network Manager or Headteacher.

USB data devices ("memory sticks") are ubiquitous – a convenient method of storing and transporting information – however they are inherently insecure and easily stolen or lost. While computers in school will forcibly encrypt all USB memory devices to ensure data stored on them is securely protected, staff should be aware it may still be possible to store sensitive data on unencrypted pen drives used outside of the school environment – and are strongly advised NOT to store confidential or sensitive information on a USB memory device unless the device itself has been encrypted.

Disciplinary or legal action may be brought against a member of staff who knowingly stores confidential or other sensitive information related to the school, students or other members of staff in an insecure manner on such a device, then loses it.

For advice about encryption or the transfer of sensitive information, staff should refer to the Network Manager.

The Internet email facility is not a secure way of transmitting confidential, sensitive or legally privileged information unless there are special security measures (such as encryption). Without these security measures, Internet email is as insecure as a postcard sent through the normal post. Staff should make sure that the Internet is suitable for transmitting information that they feel is confidential, sensitive or legally privileged. If anyone is allowed to see this type of information without permission, the member of staff may be breaking the law.

If staff have no alternative but to transmit any email over the Internet that may contain confidential, sensitive or legally privileged information, no matter what special security measures are taken, all staff are strongly advised to include the following disclaimer at the top of the E-mail where it can be read first.

'This document should only be read by those persons to whom it is addressed and is not intended to be relied upon by any person without subsequent written confirmation of its contents.

Internet communications are not secure and therefore The Long Eaton School do not accept legal responsibility for the contents of this message. Any views or opinions presented are solely those of the author and do not necessarily represent those of The Long Eaton School unless otherwise specifically stated.

If you have received this E-mail message in error, please notify us immediately by telephone on +44 (0)115 973 2438. Please also destroy and delete the message from your computer.

This Email message has been scanned for the presence of computer viruses. However, it is the responsibility of the recipient to ensure that the onward transmission, opening or use of this message and any attachments will not adversely affect its systems or data. In order to ensure this, please carry out such virus and other checks as you consider appropriate.'

This disclaimer can be set using the 'autosignature' facility where this is available. Further information on this facility is available from the Network Manager.

When disposing of material containing potentially sensitive information, due regard must be given to the sensitivity of the respective information. Any printed material containing such information regarding students or other members of staff must be shredded.

All staff should ensure that wherever possible their computer screen cannot be viewed by persons not authorised to see displayed information, and that their computer is not left logged on or in an "unlocked" state when unattended.

The Long Eaton School

Staff IT security and usage policy

Access to E-mail and Internet services

The school email and Internet facilities are for business use but The Long Eaton School will allow staff to use them privately, as long as it is reasonable. An example of what the school considers "reasonable" could be the use of internet facilities to quickly check the weather, a bus timetable or reading local news during a break or after working hours.

Conversely "unreasonable" use could be considered as any private internet or email use that is allowed to be a distraction to the role, is classed as a data or child protection issue, contravenes copyright legislation or threatens the security of the network in any way.

If staff use these facilities, they must keep to and not break any of the conditions in this policy under any circumstances.

The school has the right to monitor email and Internet use to ensure the integrity of the system and the school's obligations under the data protection act are maintained - and will take any action necessary to ensure the security of the data stored within.

If a member of staff was to intentionally access a computer system or information without permission, they are breaking the law under the Computer Misuse Act 1990.

All staff are expected to maintain the good reputation of the School when using the Internet and eMail facilities, and all need to be aware that these services are open forums subject to public scrutiny.

Use of social networking Internet sites

Staff are advised that a highly cautious approach should be taken when using social interaction sites such as Facebook. The rapid growth and take-up of these technologies has blurred the distinction between personal and professional life.

Students can, and do, actively search out teaching staff names on such sites and as a result personal comments or photographs posted there may be taken out of context, misinterpreted or even deliberately used against the member of staff leading to situations that are professionally undesirable and personally awkward.

It is recommended that staff using social networking sites should:

- *Be mindful of any image posted by them or containing them, or posting comments that may reflect negatively on their professional status as a trusted person who works with young or vulnerable people.*
- *Ensure their profile privacy settings are set to high and restrict the visibility of the bulk of their profile to approved contacts only. This is also recommended advice in guarding against personal identity theft.*
- *Register and post under a pseudonym or modified name that will not immediately be linked to them by a casual search*
- *Not encourage students to look for or attempt to contact them via social networking sites, and not add students to "friends" or other contact lists. Any such contact attempts should not be responded to.*

Access to social networking sites will not be permitted from the school network except to investigate any suspected e-Bullying or other child-protection incident.

All staff are expected to maintain the good reputation of the School when using social media or other networking sites – even in their own time - and all need to be aware that like email, these services are open and subject to public scrutiny. Any member of staff who posts comment that may be seen to be defamatory by clients, suppliers or other third parties linked with the School may be considered to have broken this policy and be subject to disciplinary action as a result.

The Long Eaton School

Staff IT security and usage policy

Email good practice

Sending official email from a personal email address, or communicating with students using their personal email accounts could lead to situations that are undesirable or uncomfortable from a professional perspective.

In order to ensure all staff remain protected when using email to communicate with parents and students, the school recommends that they:

- *Always use their school-provided email accounts for official communication – especially to parents.*
- *Only send email to students at their registered school address, avoiding the use of any personal email addresses. Students have access to the school email system from any Internet-connected PC – as such there should never be any need to send email to a student's personal account and to do so could be misinterpreted.*

Passwords

The only person staff should ever release their password to, if requested to do so, is the Headteacher. Staff are instructed not to tell anyone else their password without the Headteacher's explicit confirmation, even if requested over the telephone, no matter how genuine the caller or reason may seem.

The only person who can request that the password of a staff member be changed in their absence is the Headteacher.

Staff must not use their account details to log any other person onto the computer facilities. All access is audited and staff will be held responsible for anything done under the context of their account – whether by them or another person.

The school network is set up such that staff have to change their main Windows password every 45 days. The password change mechanism will look for a secure password: one that has a minimum of 6 alpha/numeric characters that include a mix of upper and lower case text and either a number or extended character – an example of the format might be "Passw0rd" or "Password!"

Chosen passwords should not be obvious or guessable, e.g. surname; date of birth, pet or children's names.

It is strongly advised that staff never write passwords down although in certain circumstances recording a password may be acceptable providing it is stored securely (for instance, for disaster recovery purposes). If a member of staff suspects that someone else knows their password, they must change it immediately, with assistance from IT support staff if required.

Computer viruses

It is a crime to deliberately introduce a computer virus, under the Computer Misuse Act 1990. Staff must not use the school IT, email or Internet facilities for:

- *intentionally accessing or transmitting computer viruses or other damaging software; or*
- *intentionally accessing or transmitting information about, or software designed for, creating computer viruses.*

All staff must scan any material received or downloaded from the Internet to make sure it is virus free. Automatic software is installed on all computers for this purpose and staff will be trained in its use if appropriate. Staff must not email material that has not been scanned to other users. If a virus is found, or suspected, staff are instructed to immediately stop using the computer and request advice from the Network Manager.

Staff should always follow the instructions that the Network Manager gives in relation to virus attacks or other security issues. Virus warnings from any source other than the Network Manager must only be forwarded onto the Network Manager who will then confirm its validity and decide on the next course of action.

If staff are unsure how to use the virus protection system, they must get advice from the Network Manager.

Recording usage

Staff should be aware that use of The Long Eaton School's facilities is audited to help the school ensure that the integrity of the system is maintained. This includes the recording of all internet sites accessed and monitoring of email. This is covered under the Telecommunications (Lawful Business Practice)(Interception of Communications) regulations 2000.

If staff inadvertently access an Internet site containing prohibited material, they must break the connection immediately and report it to the IT Network Manager. Failure to do this may result in disciplinary action being taken.

Staff should protect themselves by not allowing unauthorised people to use a computer or access the Internet with their logon.

Copyright

It is illegal to break copyright protection. Copyright could be broken if staff download or transmit protected material through email or over the Internet. This can include pictures from websites or MP3 music files, even if downloaded to a computer from a personal MP3 player.

Staff should not attempt to store any form of copyrighted information (including but not limited to music or video footage) using IT facilities without obtaining prior approval from the copyright holder first.

Staff must not:

- *transmit copyright software from their computer to the Internet or allow any other person to access it on their computer through the Internet; or*
- *knowingly download or transmit any protected information that was written by another person or organisation without getting permission from the owner.*
- *Store any copyright protected information using the IT facilities without first seeking the permission of the copyright holder.*

Similarly, software is also protected by copyright acts and patents and staff are advised NOT to attempt to install software themselves. This includes seemingly innocuous "free" software from the Internet. By doing so staff may be in violation of a licence agreement or be introducing "Trojan horse" software that could damage the integrity of the network or files.

If staff require additional software loading, requirements should be passed to the Network Manager who will then check the appropriate licensing agreements and arrange the installation as appropriate.

All software must be used strictly in accordance with the terms of its licence and may only be copied if specifically approved by the Network Manager. School software may not be used on any other computer without express permission beforehand.

Other security

Staff must not use or try to use the school facilities for:

- *accessing or transmitting information about, or software designed for, breaking through security controls on any system;*
- *breaking through security controls on any system; or*
- *accessing, without permission, any email that is not for them, even if it is not protected by security controls.*

Staff must exercise extreme vigilance towards any suspicious event relating to IT use and immediately report any suspected or actual breach of IT security to the Network Manager or, in exceptional cases, the Headteacher, Chair of Governors or Internal Audit.

Disaster Recovery

Although The Long Eaton School takes great care to protect the data stored on the computer systems through the deployment of fault-tolerant systems and by making daily backups of data, limited resources available to the School mean every eventuality cannot be planned for.

To ensure the continued availability of the School's computer network, and the data stored on it, the IT support department have produced a "disaster recovery plan" which details suppliers, equipment and guidelines for the restoration of the network in the event it is incapacitated.

Copies of which are held with the Business Manager and Network Manager respectively. If the plan is invoked, the Network Manager or Headteacher will advise staff accordingly and give further instruction.

Appendix B – Student ICT Code of Conduct

ICT Code of Conduct

Use of computers:

I will:

- only enter an ICT suite or use a classroom computer with permission from a member of staff.
- use all equipment sensibly.
- not eat food or drink whilst in an ICT suite or using a computer.
- not attempt to move, or unplug any of the equipment without express instruction from a member of the ICT Systems Team, and report any damage to a member of the ICT Systems Team *immediately*.
- treat the equipment with respect, as if it were my own.
- not attempt to install to, change or remove software from, the computer.
- only use the computer network to complete appropriate work.
- only use software and other programs, email and Internet to help support my education and research.

Computer Network Security:

I will:

- only access the computer network using my own authorised Username and Password.
- not tell anyone my username or password – *I understand I am responsible for anything that is done on a computer with my username, and I will face the consequences for it*.
- change my password regularly, and tell my teacher or the Network Manager if I think another student has been logging into my user account.
- not attempt to log on to another students computer area, or tamper with their work when they are logged on.
- not attempt to breach the security systems of the schools computer network.

Keeping myself safe using computing devices:

I will:

- not use the computer facilities or my mobile phone to send bullying messages or upset others
- not give my home address or phone number to anyone online or arrange to see someone I have never met via the internet without the knowledge and approval of my parents or teacher.
- help to protect myself and other students by reporting anything I see on a computer or mobile phone that I am unhappy with or if I receive messages I do not like. I understand what I say will remain confidential.
- not search the Internet for, or send/receive emails or other messages that contain pornographic, unethical or illegal requests, or any other inappropriate use which is likely to cause offence.
- not attempt to use public chat rooms without the knowledge and approval of my parents or teacher.

Monitoring of the Computer Network, E-mail and Internet Use:

In order to ensure the security of the computer network and the Health and Safety of students, the School will exercise its right by electronic means to monitor the use of the school computer systems.

This includes, but is not limited to, the monitoring of;

- *web sites,*
- *printer usage,*
- *interception of E-mails,*
- *the deletion of inappropriate materials, and*
- *the storing of text, imagery or multimedia files which are unauthorised or unlawful.*

Computer misuse will earn you a ban from using the network or internet!

Appendix C – Parental consent for Internet access form

Internet and Electronic Mail Permission Form

We are pleased to offer students of The Long Eaton School access to the computer network for electronic mail and the Internet. To gain access to email and the Internet, all students under 18 must obtain parental permission and must sign and return this form to Mr Atkinson, the ICT Network Manager.

Access to email and the Internet will enable students to explore thousands of libraries, databases, and bulletin boards while exchanging messages with Internet users throughout the world. It is a limitless educational resource however families should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. While our Internet access in school is filtered and "safe", students may find other ways in which to access offensive or inappropriate material and may come into contact with third parties who may wish them harm while doing so.

We believe that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. To mitigate against the risks presented to young or vulnerable people by widespread access to the Internet through computers or games consoles and mobile devices such as smartphones or tablets, we have an ongoing commitment to Online Safety education – making students aware of the risks they face and teaching them how to avoid them.

However, ultimately, parents and carers of children under 18 are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, The Long Eaton School supports and respects each family's right to decide whether or not to apply for access.

Parent or Guardian Agreement

Please tick the appropriate box

No, I **do not** wish my child to have Internet and email access at school [ ]

Yes, I **agree** to my child having Internet and email access at school [ ]

I hereby release the school, its personnel, and any institutions with which it is affiliated, from any and all claims and damages of any nature arising from my child's use of, or inability to use, the school's access to its network and Internet, including, but not limited to claims that may arise from the unauthorized use of the system to purchase products or services.

I will instruct my child regarding any restrictions against accessing material that are in addition to the guidance set out in rules overleaf and irrespective of the decision indicated above, I will endeavor to supervise any internet access at home to support the school's Online Safety policy. I will emphasize to my child the importance of following the rules for personal safety.

Signed: _____ _____ **Parent/Carer**

Student Agreement

Signed: _____ **Form:** _____

I have read the ICT Code of Conduct and I agree to follow the rules. Copies of the policy are posted in all computer areas and I understand that if I violate the rules my network or Internet access could be suspended and I may face other disciplinary measure

Important contact details –

Headteacher – Richard Peel
DSL – Tom Worn (Assistant Headteacher)
CPO – Karen Harrowing
Online Safety Officer – Simon Patrick
Student Wellbeing office – Kay Coxon
Network Manager – Matthew Atkinson

Tel: 0115 9732438
Email : info@longeaton.derbyshire.sch.uk