LUTTERWORTH HIGH SCHOOL

e-SAFETY POLICY

Reviewed: By the Full Governing Board

Adopted: By the Governing Board 18th June 2024

Signed: Chair of Governors: Janet Price-Jones

Date: 18th June 2024

Signed: Headteacher: Julian Kirby

Date: 18th June 2024

Review date: June 2027

Version:

Policies linked to:

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Janet Jones.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix A)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, eServices manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix C contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

3.4 The eServices manager

The eServices manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- The reporting of incidents of cyber-bullying to DSLs in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix A), and ensuring that students follow the school's terms on acceptable use (appendix A)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix A)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix A).

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum:

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships and sex education and health education in secondary schools

In **Key Stage 3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content

- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or and school newsletter. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/form teacher will discuss cyber-bullying with their tutor groups and PSHE classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

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

Any searching of students will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendix A). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

The school uses Smoothwall to monitor and report on to DSLs any activities in school which may trigger a safeguarding concern. This is supported with the use of MyConcern to record safeguarding incidents.

More information is set out in the acceptable use agreements in appendix A.

8. Students using mobile devices in school

Students may bring mobile devices into school, but are not permitted to use them during:

- Break and Lunchtime
- Before or after school on school site
- Clubs before or after school, or any other activities organised by the school
- In toilets or corridors

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendix A).

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time

- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix A.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice Sam Hill, eServices Manager.

10. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure students can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputy DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety, this is through Smoothwall and MyConcern.

This policy will be reviewed every year by Amy Hunter and Aaron Mehta. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff Code of Conduct A
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix A

ICT Acceptable Use Policy

Student ICT Acceptable Use Policy

This acceptable use policy is about ensuring that you, as a student at Lutterworth High School can use the internet, email and other technologies available at the school in a safe and secure way. This policy also seeks to ensure that you are not knowingly subject to identity theft, that you avoid cyber-bullying and just as importantly, you do not become a victim of abuse. We have banned certain sites, because they put you and the school's network at risk. Help us, to help you, keep safe.

All students at Lutterworth High School are expected to use the ICT facilities in accordance with the terms listed below. Violation of the terms outlined in this document may lead to disciplinary action.

Please read this document carefully and sign and date it to indicate your acceptance of the Policy.

- The use of any school equipment for inappropriate reasons is unauthorised.
- You should only use the Internet and e-mail services to assist you in your studies or with the permission of your class teacher.
- Computer equipment and other electronic devices should be treated with respect at all times.
- You should not attempt to install any software on any school computer or electronic device.
- You should avoid using removable storage devices such as flash drives/portable hard drives wherever possible and instead use Google Drive/OneDrive for file transfer. Should you need to use removable storage, these must be password protected/encrypted. You must always ask permission from your teacher before using removable storage devices such as flash drives.
- You must not remove network cables or attempt to connect to fixed network points without permission. This includes using your own laptops in school.
- Food and drink should not be consumed in the computer rooms or whilst working on a computer in a teaching area.
- You should not reveal your passwords to another user or try to gain access to any other user's area.
- Passwords should be a minimum of 15 characters long and contain a mixture of alphabetical, numeric and special characters. The use of three random words is advised also. Personal use passwords must not be used for any school accounts under any circumstances. The use of a password manager is encouraged.
- Lutterworth High School provides a number of services that are accessible using any device with an Internet connection. You should never leave your device logged in to any of the school's systems unattended (lock it or log out).
- You should not send email that is likely to cause any offence to either the recipient or another person.
- You should not attempt to use the Internet to access unsuitable information.
- You should not use the Internet for accessing public bulletin boards, newsgroups or chat services.
- You should not use the Internet for any commercial purposes such as buying goods or obtaining services.
- Copyright and intellectual property rights should be respected at all times.
- You should not misrepresent yourselves or another person or bring the name of Lutterworth High School into disrepute.
- You should not use the computers for commercial gain, gambling, political or advertising purposes.

- Anonymous messages and chain letters and emails should not be sent or forwarded.
- Email should be written carefully and politely. Email messages are best regarded as public property.
- You should inform a member of staff immediately if you receive any email with which you feel uncomfortable or unhappy.
- You should never make contributions to a blog, tweet, social networking site or any other online forum that is sponsored, initiated or otherwise promoted by the school which could lead to the breakdown of relationships or damage to the reputation of the school and its staff.
- If using a personal mobile device in school, you must have a robust and appropriate cover to protect the mobile device as the school cannot take responsibility for loss / damage for the mobile device in or out of school.
- The mobile device must not be used at any time during school without a teacher's supervision. You should not leave your mobile device on view or unattended at any time.
- Please ensure that the personal mobile device is locked with a passcode. This is good practice and further security for your mobile device.
- If you wish to download Apps with a cost implication you cannot expect reimbursement for the cost from the school.

The consequences of abusing this contract may result in disciplinary action. Lutterworth High School reserves the right to inspect any email account or logon account provided for use by you and to monitor all use of email and Internet facilities. The Internet service is filtered so that unsuitable information is not readily available.

STUDENT

I understand and agree to the provisions and conditions of this agreement. I understand that any disobedience to the above provisions may result in disciplinary action and the removal of my privileges to access ICT facilities. I also agree to report any misuse of the system to a staff member and I understand that misuse may come in many forms but may be viewed as any messages sent or received that indicate or suggest pornography, unethical or illegal activities, racism, sexism, inappropriate language, any act likely to cause offence.

Name: _____

Signature: _____

Date: _____

PARENT / CARER

I have read this agreement and understand that access to ICT facilities is designed for educational purposes. I understand that, whilst the Internet service provider operates a filtered service, it is impossible for Lutterworth High School to restrict access to all controversial materials and will not hold the school responsible for materials acquired on the network. I also agree to report any misuse of the system to the school. I hereby give my permission to Lutterworth High School to permit my child access to ICT facilities.

Name: _____

Signature: _____

Date: _____

Appendix A

ICT Acceptable Use Policy

This acceptable use policy is about ensuring that you, as a member of staff at Lutterworth High School can use the internet, email and other technologies available at the school in a safe and secure way. This policy also seeks to ensure that you are not knowingly subject to identity theft, that you avoid cyber-bullying and just as importantly, you do not become a victim of abuse.

All members of staff at Lutterworth High School are expected to use the ICT facilities in accordance with the terms listed below. Violation of the terms outlined in this document may lead to disciplinary action in accordance with the Leicestershire County Council disciplinary procedures for local government services employees.

Please read this document carefully and sign and date it to indicate your acceptance of the Policy.

- The use of any school equipment for inappropriate reasons is unauthorised.

- The eServices Manager/eServices Team and Senior Leadership team reserve the right to access files, folders, network data and workstations at any time, with reasonable cause.

- I understand that my use of the information systems, internet and email may be monitored and recorded to ensure policy compliance.

- Lutterworth High School provides a number of services that are accessible internally and externally, using any computer with an internet connection. You should never leave your computer logged in to any of the school's systems unattended (lock it or log out).

- Password security is vital. If you believe that your password is known by a student or other member of staff, change it immediately.

- Passwords should be a minimum of 15 characters long and contain a mixture of alphabetical, numeric and special characters. The use of three random words is advised also. Personal use passwords must not be used for any school accounts under any circumstances. The use of a password manager is encouraged.

- You should not reveal your passwords to another user or try to gain access to any other user's area.

- If you are using a computer in a classroom connected to a projector, please be aware that any student information you display on your screen may also be displayed if the projector is turned on. To ensure protection of sensitive data, please ensure that projectors are turned off, do not disturb mode is used, or that you freeze the screen effectively before accessing such information.

- If you are working at home and connect remotely to any of the school's systems, then all of the above considerations also apply. Staff must ensure that their home internet connection is secure from outside access particularly if a wireless network is used.

- For accessing email, school remote desktop provision, and other cloud services, staff will be required to setup multi-factor authentication (MFA) paired to their personal mobile device.

- You should not attempt to install software on any computer or electronic device belonging to Lutterworth High School, without the permission of the school's network manager.

- When accessing email, you will not open unknown email attachments from unknown senders. If you have any concerns about the provenance of an email, do not open it, rather delete it and report it to eServices.

- Staff members wishing to set up a personal device to receive school email and any other services provided by LHS should ensure that the device is not accessible to anyone else (e.g. family members) or left unattended. It is strongly recommended that a separate application / device user account is used for

accessing school emails/services (e.g. Microsoft Outlook) to ensure that they are kept separate from personal and family accounts. Appropriate security (strong passwords, and multi-factor authentication (MFA) or biometric protection) must be used to ensure accounts and the personal device remains secure. Any loss or theft of a personal device that grants access to a school email account or any other service provided by LHS should be reported immediately to eServices.

- You will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act, and in accordance with the school's GDPR policy. This means that all personal data will be processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in school, hosted online or accessed remotely. Any data which is being removed from the school site (such as via email, USB stick, portable hard drives) will be encrypted, and the use of the school cloud platforms should be used. Any images or videos of pupils will always take into account parental consent. You will ensure that when data is no longer needed this will be effectively deleted or placed in the confidential waste bins provided throughout the school. No data should be stored on personal cloud accounts.

- You will report all incidents of concern regarding children's online safety to the designated safeguarding lead and/or the e-safety officer as soon as possible. You will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable/extreme websites to the e-safety coordinator.

- You will report any loss or damage to school provided ICT equipment to the eServices Manager immediately.

- Be responsible with the amount of storage space used, and undertake regular 'housekeeping' to delete unwanted files when requested.

- You should avoid using removable storage devices such as flash drives/portable hard drives wherever possible and instead use Google Drive/OneDrive for file transfer between school and home. Should you need to use removable storage, these must be password protected/encrypted.

- You will only transport, hold, disclose or share personal information about others, as outlined in the school GDPR policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based, Protected and Restricted data must be held in lockable storage.

- Printers are provided across the school for work-related use only.

- Be aware that if you install software on a home computer which is licensed through the school, it is your responsibility to uninstall it when you leave the school's employment.

- You must not remove network cables or attempt to connect to network points without permission.

- You should not send email that is likely to cause any offence to either the recipient or another person.

- Copyright and intellectual property rights should be respected at all times.

- You should not use the computers in school for commercial gain, gambling, political or advertising purposes.

- Anonymous messages and chain letters should not be sent or forwarded.

- Email should be written carefully and politely. Email messages are best regarded as public property. If you access school data, including emails, SIMs, Teams, OneDrive, Edulink, and Drive etc. via a personal mobile device a password must be used.

- You should inform a member of the SLT immediately if you receive any email with which you feel uncomfortable or unhappy.

- You should never repeat or publish confidential information on social networking sites. When using social networking sites never invite or accept friendship requests from current or prior students from Lutterworth High School. This also includes any other form of personal electronic media.

- You should never make comments on social networking sites which could lead to the breakdown of relationships in the workplace or damage to the reputation of the school and its staff. This includes making personal comments that could be detrimental to your professional status.

- If you leave the school, you must return any IT equipment assigned to you unlocked, and unencrypted to the eServices Office before you leave. This includes but is not limited to laptops, iPads, Chromebooks, phones and memory devices etc. This also applies to personal devices in the event of exchanging, upgrading, gifting or selling a device or termination of employment, that any school data/accounts present on all personal devices will be securely deleted.

- I understand and agree to the provisions and conditions of this agreement. I understand that any violations of the above provision may result in disciplinary action and revocation of privileges. I also agree to report any misuse of the system to a member of the SLT. I agree to use the internet and electronic communications systems in compliance with the terms outlined in this document and understand that my internet access and any electronic communications may be logged or monitored.

- I understand and agree to the provisions and agreements of this policy, and also agree to the following school IT policies -

  - LHS Remote Access Policy
  - LHS Secure Configuration Policy
  - LHS Access Control Policy
  - LHS Anti-Malware Ransomware Policy
  - LHS Information Security Policy
  - LHS Password Policy
  - LHS eSafety Policy
  - LHS Social Media Policy
  - LHS Web Filtering Policy

Name: _____

Signature: _____

Date: _____

Appendix B

Risk Log

No.	Activity	Risk	Likelihood	Impact	Score	Owner
1	Internet browsing	Access to inappropriate/illegal content - staff	1	3	3	EServices Manager/ e-safety Officer
2	Internet browsing	Access to inappropriate/illegal content - students	2	3	6	EServices Manager/ e-safety Officer/Tutors
3	iPads/laptops	Downloading school data onto iPads/laptops	2	3	6	EServices Manager/ e-safety Officer
4	USB Memory sticks	Use of non-encrypted memory sticks that carry school data	3	3	9	EServices Manager/ e-safety Officer
5	Twitter	Inappropriate comments	1	3	3	EServices Manager/ e-safety Officer
6	Mobile phones	Access to inappropriate/illegal content – students	2	3	6	EServices Manager/ e-safety Officer
7	Mobile phones	Inappropriate use eg. taking photo's, texting etc.	2	3	6	E-safety Officer/Tutors
8	School owned devices	Loss or damage to school owned devices	1	3	3	EServices Manager/ e-safety Officer

Likelihood: **How likely is it that the risk could happen (forseeability).**
Impact: **What would be the impact to the school (eg. this could be in terms of legality, reputation, complaints from parents, reporting in the press etc.)**
Likelihood and Impact are between 1 and 3, 1 being the lowest. Multiply Likelihood and Impact to achieve score.
LEGEND/SCORE: **1 – 3 = Low Risk**
4 – 6 = Medium Risk
7 – 9 = High Risk
Owner: **The person/s who will action the risk assessment and recommend the mitigation to Headteacher and Governing Body. Final decision rests with the Headteacher and Governing Body**

Appendix C: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways students can abuse their peers online?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for students and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	