LUTTERWORTH HIGH SCHOOL

e-SAFETY POLICY

Reviewed: By the Health and Safety Committee

Adopted: By the Governing Body – 08/10/19

Signed: Chair of Governors: Janet Jones

Date: 8th October 2019

Signed: Head Teacher: Julian Kirby

Date: 8th October 2019

Review Date: 10/2021

LUTTERWORTH HIGH SCHOOL e-SAFETY POLICY

Table of Contents

Introduction

Model Policy

Policy Statement

Policy Governance - Roles/responsibilities

Governing Body
Headteacher
e-Safety Officer
ICT Technical Support Staff
All Staff
All Students
Parents and Carers
e-Safety Committee

Technology

Internet Filtering
Email Filtering
Encryption
Passwords
Anti-Virus

Safe Use

Internet
Email
Photos and videos
Social Networking
Incidents
Training and Curriculum
Related Policies

Appendix A - Acceptable Use Policy (Students, Staff, GPT Students and Governors)

Appendix B - E-Safety Incident Log

Appendix C - Risk Assessment Log

Appendix D - Inappropriate Use Flowchart

Appendix E - Illegal Use Flowchart

Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users – refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school eg. parent, guardian, carer.

School – any school business or activity conducted on or off the school site eg. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents, any bodies or persons hiring the school premises.

Safeguarding is a serious matter; at Lutterworth High School (LHS) we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- 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 the LHS website; upon review all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use Policy. A copy of this policy will be sent home with students at the beginning of each school year with a permission slip. The Students Acceptable Use Policy is included within the Students' Personal Organiser, signed at the beginning of each school year and checked by the form tutor. 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. Records of the above will be held centrally by the e-Safety Officer.

Policy Governance (Roles & 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 e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure 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 in regards to training, identified risks and any incidents.
    - Represent e-Safety at the Health and Safety Committee

Headteacher

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

The Headteacher will ensure that:

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

e-Safety Officer

The day-to-day duty of e-Safety Officer is devolved to Amy Hunter.

The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize herself 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.
- Ensure the process and procedures of LHS policies eg. child protection, behaviour management, information security and acceptable use policies correlate with this e-Safety policy.
- Advise the Headteacher, governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering hardware / software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

eServices Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any e-safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Headteacher.
    - Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 10 characters including capital letter, special character and a number. Password will be set to expire every 45 days.
    - The IT System Administrator password is to be changed on a monthly (30 day) basis.

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.
- Any e-safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made), or in her absence to the Headteacher. If you are unsure the matter is to be raised with the e-Safety Officer or the Headteacher to make a decision.
- The reporting flowcharts contained within this e-safety policy are fully understood.

All Students

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

e-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. 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 school letters with content specific the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy (within the Students' organiser) before any access can be granted to school ICT equipment or services.

Health and Safety Committee

The e-Safety Officer is a member of the Health and Safety Committee. E-Safety is a mandatory item on the Agenda and the e-Safety Officer is responsible:

- for advising on changes to the e-safety policy.
- for establishing the effectiveness (or not) of e-safety training and awareness in the school.
- for recommending further initiatives for e-safety training and awareness at the school.

The Health and Safety Committee meet on a termly basis.

Technology

LHS uses a range of devices including PC's, laptops, Apple ipads and mobile phones. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – Our ISP (KCOM) provides our managed firewall service to prevent unauthorized access to illegal websites. We use the Lightspeed Rocket (hardware) webfilter as an inline proxy to prevent access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ICT Coordinator, e-Safety Officer and IT Support 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 O365 (OVS Educational plan) to host our emails in Azure. This includes the service that prevents any infected email to be sent from the school, or to be received by the school as much as possible. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data. Other forms of malicious email i.e. phishing emails are controlled via policy and training and awareness.

Encryption – All school devices that hold personal data (as defined by the GDPR Act May 25th 2018) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the
Information Commissioner's Office. For more information please see the LHS Information Security Policy.

Passwords – all staff and students will be unable to access any device without a unique username and password. Staff and student passwords will change on a termly basis, after a set number of days or if there has been a compromise, whichever is sooner. The ICT Coordinator and IT Support will be responsible for ensuring that passwords are changed.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as keydrives) are to be scanned for viruses before use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use Policy; students upon signing and their acceptance of the Acceptable Use Policy.

Email – Emails of a personal nature are permitted. However, all staff are reminded that emails are subject to Freedom of Information requests (SAR – Subject Access Request) and therefore staff should ensure that emails are polite and carefully written and not make personal comments that could be detrimental to their professional status or damage the school reputation. If staff access school data, including emails, SIMS, TEAMS etc. via a personal mobile device a password must be installed on that device.

Students are permitted to use the school email system, and as such will be given their own email address. The email address will be made up of their first name and first initial of their surname, e.g. org.

Photos and videos – The school permits photos and videos to be taken by staff and students. Staff should only take photographs or videos of students with the express permission of students (if the student is 13 or over) or with parental consent (for students younger than 13). This is normally obtained from parents on entry to the school via the' Curriculum Led Activities Form of Consent' and a list of the students whose parents have objected to this is kept by the Health and Safety Officer. It is preferred that school equipment is used for this, but in any case, images must be transferred within a reasonable time scale and solely to the school's network or hosted services controlled by the school and deleted from the original device.

Students must be advised when using their personal digital equipment, especially during field trips, that images and video should only be taken with the subjects' consent. Students should also be advised that complaints against this condition will be considered a serious breach of this policy and risk having the device confiscated until it can be inspected, in their presence, by the e-safety officer or a member of the Senior Leadership Team.

Social Networking – There are many social networking services available; LHS is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. Twitter is permitted for use within LHS and has been appropriately risk assessed; should staff wish to use other social media; permission must first be sought via the e-Safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Twitter – used by the school as a broadcast service (see below).

A broadcast service is a one-way communication method in order to share school information with the wider school community. Via facebook. Staff are encouraged to collaborate and engage in academic discussions, via Twitter therefore, students will be encouraged to follow staff's professional account two-way communication must be transparent and be directed to the conversation. No political conversation or conversation that could put the school's reputation at risk must be allowed. If any incidences do occur this must be reported to the eSafety office, Amy Hunter
In addition, the following is to be strictly adhered to:

- There is to be no identification of students using first name and surname; first name only is to be used. And never upload a photo and a name
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence, which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the school's attention that there is a resource, which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in his/her absence the Headteacher. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, LHS will have an annual programme of training which is suitable to the audience.

e-Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

As well as the programme of training, we will establish further training or lessons as necessary in response to any incidents.

Review Date: 10/2021

The e-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

The e-Safety Training Programme can be found on the school website www.lutterworthhigh.co.uk under the "e-Safety" link.

Related Policies, Procedures and useful Information

The following Lutterworth High School policies and procedures can be found on the school website www.lutterworthhigh.co.uk within the 'Information' header.

Information Security Policy
Mobile Phone Usage Policy
Acceptable Use Policy
Anti-Bullying Policy
Behaviour Management Policy

See our 'E-Safety' page on our website http://www.lutterworthhigh.co.uk/e-safety/ for more information and useful websites.

Appendix A

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 proxy sites as well as anonymous proxy 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 terms outlined in this document may lead to loss of access and / or 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 your own software on any computer or electronic device.
- 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.
- 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.
- Copyright and intellectual property rights should be respected at all times.
- You should not use the Internet for any commercial purposes such as buying goods or obtaining services.
- You should not misrepresent yourselves or another person or bring the name of Lutterworth High School into disrepute through using the computers.
- You should not use the computers 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.
- 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.

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: _____

Review Date: 10/2021

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. We have had to ban certain proxy sites as well as anonymous proxy sites, because they put the school network at risk.

All members of staff at Lutterworth High School are expected to use the ICT facilities in accordance with the terms listed below. Violation of terms outlined in this document may lead to disciplinary action in accordance with 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.
- 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.
- 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 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.
- 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.
- You should avoid using removable storage devices such as flash drives whenever possible and instead use the TEAMS for file transfer between school and home.
- Printers are provided across the School for work-related use only.
- You must not remove network cables or attempt to connect to fixed 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 etc. via a personal mobile device a password must be installed.
- 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 past students from Lutterworth High School. This also includes any other form of personal electronic media.
- 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. This includes making personal comments that could be detrimental to your professional status.

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.

Name: _____

Signature: _____

Date: _____

Appendix A

ICT Acceptable Use Policy

This Acceptable Use Policy is about ensuring that you 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 had to ban certain proxy sites as well as anonymous proxy sites, because they put the school network at risk.

All PGCE / GTP students, adults on work placements and adult volunteers based at Lutterworth High School are expected to use the ICT facilities in accordance with the terms listed below. 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.
- 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 any other adult user, change it immediately.
- 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 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.
- 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.
- You should avoid using removable storage devices such as flash drives whenever possible and instead use the TEAMS for file transfer between school and home.
- Printers are provided across the School for work-related use only.
- You must not remove network cables or attempt to connect to fixed 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 Internet in School for any commercial purposes such as buying goods or obtaining services.
- 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 etc. via a personal mobile device a password must be installed.

- 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 past students from Lutterworth High School. This also includes any other form of personal electronic media.
- 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. This includes making personal comments that could be detrimental to your professional status.

I understand and agree to the provisions and conditions of this agreement. I understand that any violations of the above provision may result in 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.

Name: _____

Signature: _____

Date: _____

Appendix A

ICT Acceptable Use Policy

All Governors of Lutterworth High School are expected to use any ICT facilities provided by the School in accordance with the terms listed below. 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.
- Lutterworth High School provides a number of services that are accessible 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 any other adult user, change it immediately.
- You should not reveal your passwords to another user or try to gain access to any other user's area.
- Copyright and intellectual property rights should be respected at all times.
- You should not send email that is likely to cause any offence to either the recipient or another person.
- Email should be written carefully and politely. Email messages are best regarded as public property. If you access school data, including emails, SIMs, TEAMS etc. via a personal mobile device a password must be installed.
- 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 past students from Lutterworth High School. This also includes any other form of personal electronic media.
- 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. This includes making personal comments that could be detrimental to your professional status.
-

I understand and agree to the provisions and conditions of this agreement. I understand that any violations of the above provision may result in revocation of privileges. I agree to use any electronic communications systems provided by the School in compliance with the terms outlined in this document and understand that my communications may be logged or monitored.

Name: _____

Signature: _____

Date: _____

Review Date: 10/2021

Appendix B

e-Safety Incident Log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, e-Safety Officer)*	
	When:	**When:**	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review:			
Signature (Headteacher)		**Date:**	
Signature (Governor)		**Date:**	

Appendix C

Risk Log

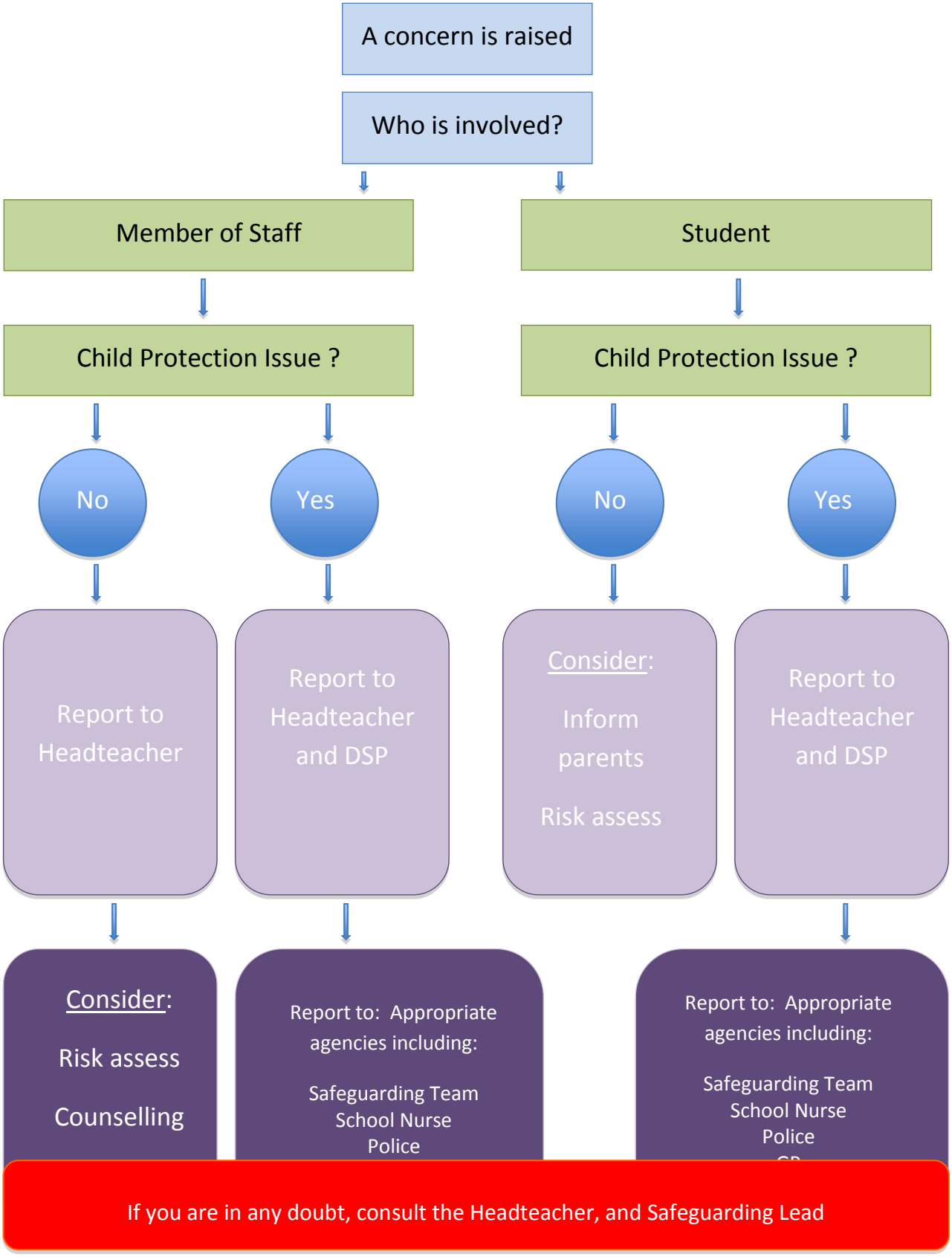
No.	Activity	Risk	Likelihood	Impact	Score	Owner
1	Internet browsing	Access to inappropriate/illegal content - staff	1	3	3	Network Manager/e-safety Officer
2	Internet browsing	Access to inappropriate/illegal content - students	2	3	6	Network Manager/e-safety Officer/Tutors
3	iPads/laptops	Downloading school data onto iPads/laptops	2	3	6	Network Manager/e-safety Officer
4	USB Memory sticks	Use of non-encrypted memory sticks that carry school data	3	3	9	Network Manager/e-safety Officer
5	Twitter	Inappropriate comments	1	3	3	Network Manager/e-safety Officer
6	Mobile phones	Access to inappropriate/illegal content – students	2	3	6	Network 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	Network 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.**

Review Date: 10/2021

Appendix D

Inappropriate Activity Flowchart



Appendix E

Illegal Activity Flowchart