LOSTOCK HALL ACADEMY

ONLINE SAFETY AND ACCEPTABLE IT USE POLICY

Date effective from	September 2024
Date approved by Trustees	July 2024
Policy Prepared by	Mr N Clitheroe, Senior Assistant Vice Principal

Contents:

Statement of intent

Lostock Hall Academy understands that using online services is an important aspect of raising educational standards, promoting student achievement, and enhancing teaching and learning. The use of online services is embedded throughout the academy; therefore, there are a number of controls in place to ensure the safety of students and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect students and staff revolve around these areas of risk. Our academy has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all students and staff.

1 Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) 'Filtering and monitoring standards for academy's and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2024) 'Keeping children safe in education 2024'
- DfE (2023) 'Teaching online safety in academy'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

2 Roles and responsibilities

The **Board of Trustees** will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up to date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant academy policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The **Principal** will be responsible for:

Ensuring that online safety is a running and interrelated theme throughout the academy's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.

Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.

Ensuring staff receive regular, up-to-date, and appropriate online safety training and information as part of their induction and safeguarding training.

Ensuring online safety practices are audited and evaluated.

Organising engagement with parents/carers to keep them up-to-date with current online safety issues and how the academy is keeping students safe.

Working with the DSL and ICT technicians to conduct half-termly light-touch reviews of this policy.

Working with the DSL and board of trustees to update this policy on an annual basis.

The **DSL** will be responsible for:

- Taking the lead responsibility for online safety in the academy.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that students with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the academy's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the academy's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by students and staff, and ensuring all members of the academy community understand this procedure.
- Understanding the filtering and monitoring processes in place at the academy.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the academy.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the academy's provision and using this data to update the academy's procedures.
- Reporting to the Board of Trustees about online safety on a termly basis.
- Working with the Principal and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the Principal and Board of Trustees to update this policy on an annual basis.

ICT technicians will be responsible for:

- Providing technical support in the development and implementation of the academy's online safety policies and procedures.
- Implementing appropriate security measures as directed by the Principal.
- Ensuring that the academy's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and Principal to conduct half-termly light-touch reviews of this policy.

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that students may be unsafe online.
- Reporting concerns in line with the academy's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Students will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from academy staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3 Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the academy's approach to online safety, with support from deputies and the Principal where appropriate, and will ensure that there are strong processes in place to handle any concerns about students' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all academy operations in the following ways:

- Staff and Trustees receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted termly on the topic of remaining safe online

Handling online safety concerns

Any disclosures made by students to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also

acknowledge that students displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents/carers to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the Principal, who decides on the best course of action in line with the relevant policies. If the concern is about the Principal, it is reported to the chair of Trustees.

Concerns regarding a student's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Principal and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.
Where there is a concern that illegal activity has taken place, the Principal/DSL contacts the police.

The academy avoids unnecessarily criminalising students, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a student has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the academy's response are recorded by the DSL.

4 Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The academy will be aware that certain students can be more at risk of abuse and/or bullying online, such as LGBTQ+ students and students with SEND.

Cyberbullying against students or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-Bullying Policy.

5 Child-on-child sexual abuse and harassment

Students may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of academy, off and online, and will remain aware that students are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a culture that normalises abuse and leads to students becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The academy will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other students taking "sides", often leading to repeat harassment. The academy will respond to these incidents in line with the Child-on-child Abuse Policy and the Social Media Policy.

The academy will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the academy premises or using academy-owned equipment. Concerns regarding online child-on-child abuse will be

reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

6 Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that students who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the student may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact students are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse.

The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the academy and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a student may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about students with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain students at increased vulnerability to radicalisation, as outlined in the Child Protection and Safeguarding Policy. Staff will be expected to exercise vigilance towards any students displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a student relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Child Protection and Safeguarding Policy.

7 Mental health

Staff will be aware that online activity both in and outside of academy can have a substantial impact on a student's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a student is suffering from challenges in their mental health. Concerns about the mental health of a student will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

8 Online hoaxes and harmful online challenges

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the student and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst students in the academy, they will report this to the DSL immediately.
The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to students, and whether the risk is one that is localised to the academy or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.
Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Principal will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing students.

- Not inadvertently encouraging students to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger students but is almost exclusively being shared amongst older students.
- Proportional to the actual or perceived risk.
- Helpful to the students who are, or are perceived to be, at risk.
- Appropriate for the relevant students' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting students at risk of harm, they will ensure that the challenge is directly addressed to the relevant students, e.g. those within a particular age range that is directly affected or individual students at risk where appropriate.

The DSL and Principal will only implement an academy-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing students' exposure to the risk is considered and mitigated as far as possible.

9 Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The academy will factor into its approach to online safety the risk that students with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a student's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and Principal will ensure that students are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

10 Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that students are at risk of abuse, by their peers and by adults,

online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

11 Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- RSHE
- PSHE
- Citizenship
- ICT

Online safety teaching is always appropriate to students' ages and developmental stages.

Students are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours students learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks students may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in appendix A of this policy.

The DSL will be involved with the development of the academy's online safety curriculum. Students will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that students who may be more vulnerable to online harms, e.g. students with SEND and LAC, receive the information and support they need.

The academy will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from students.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of students.

External visitors may be invited into academy to help with the delivery of certain aspects of the online safety curriculum. The Principal and DSL will decide when it is appropriate to invite external groups into academy and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that students in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any student who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a student who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which students feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything students raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a student makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

12 Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Intranet/Synergy
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that students use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Students will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

13 Use of smart technology

While the academy recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the academy will ensure it manages.

Students will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the academy's Technology Acceptable Use Agreement for Students.

The academy recognises that students' unlimited and unrestricted access to the internet via mobile phone networks means that some students may use the internet in a way which breaches the academy's acceptable use of ICT agreement for students.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Students will not be permitted to use smart devices or any other personal technology whilst in the classroom, unless directed by a member of staff.

Where it is deemed necessary, the academy will ban student's use of personal technology whilst on academy site.

Where there is a significant problem with the misuse of smart technology among students, the academy will discipline those involved in line with the academy's Behaviour for Learning Policy.

The academy will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The academy will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The academy will consider the 4Cs (content, contact, conduct and commerce) when educating students about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

14 Educating parents/carers

The academy will work in partnership with parents/carers to ensure students stay safe online at academy and at home. Parents/carers will be provided with information about the academy's approach to online safety and their role in protecting their children. Parents/carers will be sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it. Monthly Online Safety Newsletters will be shared with parents/carers.

Parents/carers will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of students, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents/carers will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' evenings
- Newsletters
- Online resources/Academy social media posts

15 Internet access

Students, staff and other members of the academy community will only be granted access to the academy's internet network once they have read and signed the Acceptable Use Agreement (See Appendix B). A record will be kept of users who have been granted internet access in the academy office.

All members of the academy community will be encouraged to use the academy's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

16 Filtering and monitoring online activity

The Board of Trustees will ensure the academy's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for academy's and colleges'. The board of trustees will ensure 'over blocking' does not lead to unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the academy's safeguarding needs.

The Principal and ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the academy implements will be appropriate to students' ages, the number of students using the network, how often students access the network, and the proportionality of costs compared to the risks. ICT technicians will undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the Principal. Prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a student has deliberately breached the filtering system, they will be disciplined in line with the Behaviour for Learning Policy. If a member of

staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The academy's network and academy-owned devices will be appropriately monitored. All users of the network and academy-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

Below are links to DfE and UK Safer Internet Centre for guidance on filtering and monitoring:

https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges

https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring

17 Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT technicians. Firewalls will be switched on at all times. ICT technicians will review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

Staff and students will be advised not to download unapproved software or open unfamiliar email attachments and will be expected to report all malware and virus attacks to ICT technicians.

All members of staff will have their own unique usernames and private passwords to access the academy's systems. All students will be provided with their own unique username and private passwords. Staff members and students will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers, and symbols to ensure they are as secure as possible. Passwords will expire after 90 days, after which users will be required to change them.

Users will inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the Principal will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

18 Emails

Access to and the use of emails will be managed in line with the Data Protection Policy, IT Acceptable Use Agreement.

Staff and students will be given approved academy email accounts and will only be able to use these accounts at academy and when doing academy-related work outside of academy hours. Prior to being authorised to use the email system, staff and students must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the academy site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and students will be required to block spam and junk mail, and report the matter to ICT technicians. The academy's monitoring system can detect inappropriate links, malware and profanity within emails – staff and students will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. ICT technicians will organise an annual assembly where they explain what a phishing email and other malicious emails might look like – this assembly will include information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

19 Generative artificial intelligence (AI)

The academy will take steps to prepare students for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to students' age.

The academy will ensure its IT system includes appropriate filtering and monitoring systems to limit student's ability to access or create harmful or inappropriate content through generative AI.

The academy will ensure that students are not accessing or creating harmful or inappropriate content, including through generative AI.

The academy will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The academy will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

20 Social networking

The use of social media by staff and students will be managed in line with the academy's IT Acceptable Use Agreement.

21 The academy website

The Principal will be responsible for the overall content of the academy website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

22 Use of devices

Staff members and students will be issued with academy-owned devices to assist with their work, where necessary. Requirements around the use of academy-owned devices can be found in the academy's IT Acceptable Use Agreement.

The use of personal devices on the academy premises and for the purposes of academy work will be managed in line with the Staff ICT and Electronic Devices Policy and Students' Personal Electronic Devices Policy.

23 Remote learning

All remote learning will be delivered in line with the academy's Behaviour for Learning Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

24 Monitoring and review

The academy recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the Principal conduct half-termly light-touch reviews of this policy to evaluate its effectiveness.

The Board of Trustees, Principal and DSL will review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is September 2025.

Any changes made to this policy are communicated to all members of the academy community.

Appendix A

Online harms and risks – curriculum coverage

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching will include the following: • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm will be covered in the following curriculum areas: • Health education • Computing
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching will include the following: • What a digital footprint is, how it develops and how it can affect students' futures • How cookies work • How content can be shared, tagged and traced • How difficult it is to remove something once it has been shared online • What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm will be covered in the following curriculum areas: • RSHE • Computing
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching will include the following: • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleading information can be shared inadvertently • Misinformation and understanding that some genuine information can be published with the deliberate intent to harm, e.g. releasing private information or photographs	This risk or harm will be covered in the following curriculum areas: • RSHE • Computing • Personal Development • Citizenship

	• Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons • That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online • How to measure and check authenticity online • The potential consequences of sharing information that may not be true	
Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching will include the following: • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails • The risks of entering information to a website which is not secure • What students should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email • Who students should go to for support • The risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist	This risk or harm will be covered in the following curriculum areas: • RSHE • Computing
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching will include the following: • What identity fraud, scams and phishing are • That online fraud can be highly sophisticated and that anyone can be a victim • How to protect yourself and others against different types of online fraud • How to identify 'money mule' schemes and recruiters • The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal • The risk of sharing personal information that could be used by fraudsters • That children are sometimes targeted to access adults' data	This risk or harm will be covered in the following curriculum areas: • RSHE • Computing

	• What 'good' companies will and will not do when it comes to personal details • How to report fraud, phishing attempts, suspicious websites and adverts	
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching will include the following: • Why passwords are important, how to keep them safe and that others might try to get people to reveal them • How to recognise phishing scams • The importance of online security to protect against viruses that are designed to gain access to password information • What to do when a password is compromised or thought to be compromised	This risk or harm will be covered in the following curriculum areas: • RSHE • Computing
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching will include the following: • How cookies work • How data is farmed from sources which look neutral • How and why personal data is shared by online companies • How students can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather	This risk or harm will be covered in the following curriculum areas: • RSHE • Computing
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching will include the following: • That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible to encourage them to spend money or generate advertising revenue • How notifications are used to pull users back online	This risk or harm will be covered in the following curriculum areas: • Health education • Computing
Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching will include the following:	This risk or harm will be covered in the following curriculum areas:

	• How to find information about privacy settings on various sites, apps, devices and platforms • That privacy settings have limitations	• RSHE • Computing
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching will include the following: • How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts • How the targeting is done • The concept of clickbait and how companies can use it to draw people to their sites and services	This risk or harm will be covered in the following curriculum areas: • RSHE • Computing
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching will include the following: • The types of online abuse, including sexual harassment, bullying, trolling and intimidation • When online abuse can become illegal • How to respond to online abuse and how to access support • How to respond when the abuse is anonymous • The potential implications of online abuse • What acceptable and unacceptable online behaviours look like	This risk or harm will be covered in the following curriculum areas: • RSHE • Computing • Citizenship
Radicalisation	Students are at risk of accessing inappropriate and harmful extremist content online, including terrorist material. Extremist and terrorist groups use social media to identify and target vulnerable individuals. Teaching will include the following: • How to recognise extremist behaviour and content online • Which actions could be identified as criminal activity • Techniques used for persuasion • How to access support from trusted individuals and organisations	All areas of the curriculum
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching will include the following:	This risk or harm will be covered in the following curriculum areas:

	• What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal • How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why • That it is okay to say no and to not take part in a challenge • How and where to go for help • The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges	• RSHE
Content which incites violence	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching will include the following: • That online content (sometimes gang related) can glamorise the possession of weapons and drugs • That to intentionally encourage or assist in an offence is also a criminal offence • How and where to get help if they are worried about involvement in violence	This risk or harm will be covered in the following curriculum areas: • RSHE
Fake profiles	Not everyone online is who they say they are. Teaching will include the following: • That, in some cases, profiles may be people posing as someone they are not or may be 'bots' • How to look out for fake profiles	This risk or harm will be covered in the following curriculum areas: • RSHE • Computing
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, gangs and financial exploitation. Teaching will include the following: • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour • The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in academy and to the police At all stages, it is important to balance teaching students about making sensible decisions to stay safe whilst being	This risk or harm will be covered in the following curriculum areas: • RSHE

	clear it is never the fault of the child who is abused and why victim blaming is always wrong.	
Livestreaming	Livestreaming (showing a video of yourself in real-time online, either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching will include the following: • What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content • That online behaviours should mirror offline behaviours and that this should be considered when making a livestream • That students should not feel pressured to do something online that they would not do offline • The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next • The risks of grooming	This risk or harm will be covered in the following curriculum areas: • RSHE
Pornography	Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching will include the following: • That pornography is not an accurate portrayal of adult sexual relationships • That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour • That not all people featured in pornographic material are doing so willingly, e.g. revenge porn or people trafficked into sex work	This risk or harm will be covered in the following curriculum areas: • RSHE
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching will include the following: • That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people students do not know, or arranging to meet someone they have not met before	This risk or harm will be covered in the following curriculum areas: • RSHE • Computing

	• What online consent is and how to develop strategies to confidently say no to both friends and strangers online	
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching will include the following: • The issue of using image filters and digital enhancement • The role of social media influencers, including that they are paid to influence the behaviour of their followers • That 'easy money' lifestyles and offers may be too good to be true • The issue of photo manipulation, including why people do it and how to look out for it	This risk or harm will be covered in the following curriculum areas: • RSHE
Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching will include the following: • How to evaluate critically what students are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity • The need for students to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear or missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues • That isolation and loneliness can affect students and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help	This risk or harm will be covered in the following curriculum areas: • Health education
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching will include the following: • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressure How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	This risk or harm will be covered in the following curriculum areas: • RSHE

Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching will include the following: • Strategies for positive use • How to build a professional online profile	This risk or harm will be covered in the following curriculum areas: • RSHE
Suicide, self-harm and eating disorders	Students may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for students and should take care to avoid giving instructions or methods and avoid using language, videos and images.	

Appendix B

IT Acceptable User Agreement

LOSTOCK HALL ACADEMY

Acceptable Use Policy for the Internet and Computer Facilities

PLEASE READ AND RETAIN FOR YOUR INFORMATION

1 CONTENTS

INTRODUCTION

Use of the Internet by schools/academies is growing rapidly. The problems and issues that have been highlighted by the media concern most academy's. Whilst some of the media interest may be hype, there is real cause for concern and it is imperative that academies consider issues carefully before allowing students access, supervised or unsupervised, to the Internet.

As part of the academy's IT programme we offer students supervised access to the Internet. Lostock Hall Academy uses a filtered broadband Internet connection provided by the Local Education Authority. However, it is our belief that there is no present or future technical solution that can completely guarantee the restriction of students to unwanted Internet material. Most development work is concentrated on removing access to pornography and even here success is unlikely to become complete. Other areas of unacceptable materials, such as racist, sexist, extremist, political or violent material are sometimes beyond the scope of most safeguarding programmes. In view of this we believe parental involvement is the most sensible course of action. The development of a detailed Academy Policy and practice, together with a parent/academy contract in an "Acceptable Use Policy" is our advised action.

LETTER FROM THE PRINCIPAL

Dear Parent/Carer

As part of the academy's ICT programme we offer students supervised access to the Internet. Before being allowed to use the Internet, all students must obtain parental permission and both they and you must sign and return the enclosed form as evidence of your approval and their acceptance of the academy rules on this matter.

Access to the Internet is via the Local Education Authority and is a filtered service. This filtering is not 100% fool proof as there is always new information appearing on the screen, which manages to get through the system. 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.

Access to the Internet will enable students to explore thousands of libraries, databases and bulletin boards as well as, within reason, being able to exchange messages with other Internet users throughout the world.

Whilst our aim for Internet use is to further educational goals and objectives, students may find ways to access other materials as well. However, 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. During academy time teachers will guide students towards appropriate materials. Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of students to access inappropriate materials, the academy cannot be held responsible for the nature or content of materials accessed through the Internet. Ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the academy supports and respects each family's right to decide whether or not to apply for access.

I would be grateful if you could read the enclosed guidance documents and then complete and return the permission form at the end. If there is any further information you require, please do not hesitate to contact me.

Yours sincerely

G F Gorman
Principal

Academy Policy

2 Student access to the Internet

The academy encourages use by students of the rich information resources available on the Internet, together with the development of appropriate skills to analyse and evaluate such resources. These skills will be fundamental in the society our students will be entering.

Online services significantly alter the information landscape for academy's by opening classrooms to a broader array of resources. In the past, teaching and library materials could usually be carefully selected. All such materials would be chosen to be consistent with national policies, supporting and enriching the curriculum whilst taking into account the various teaching needs, learning styles, abilities and developmental levels of the students. Internet access, because it may lead to any publicly available site in the world, will open classrooms to electronic information resources which have not been selected by teachers as appropriate for use by students.

Electronic information research skills are now fundamental to prepare citizens and future employees during the Information Age. The academy expects that staff will further investigate possibilities and blend the use of such information as appropriate within the curriculum and that staff will provide guidance and instruction to students in the appropriate use of such resources. Staff will consult with the Senior IT Technician for advice on content, training and appropriate teaching levels consistent with the academy's ICT/Computing lessons.

Access to online resources will enable students to explore thousands of libraries, databases and bulletin boards while exchanging messages with people throughout the world. The academy believes that the benefits to students from access to information resources and increased opportunities for collaboration exceed the disadvantages. But ultimately, parents/carers are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end the academy supports and respects each family's right to decide whether or not to apply for access.

The academy's computing and DSL's will prepare appropriate procedures for implementing this policy and for reviewing and evaluating its effect on teaching and learning.

3 Resource Development

In order to match electronic resources as closely as possible to the National and Academy Curriculum, teachers will continue to review and evaluate resources in order to offer homepages and menus of materials that are appropriate to the age range and ability of the group being taught. Appropriate guidance will be given to students as they make use of telecommunications and electronic information resources to conduct research and other studies.

As much as possible, the academy's chosen information provider has organised information resources in ways that point students to those that have been reviewed and evaluated prior to use. While students may be able to move beyond those resources to others that have not been evaluated by staff, they shall be provided with guidelines and lists of resources particularly suited to the learning objective.

4 Academy Rules

The academy has developed a set of guidelines for Internet use by students. These rules will be made available to all students, and kept under constant review. All students will be informed by staff of their rights and responsibilities as users, before their first use, either as an individual user or as a member of a class or group.

STUDENT GUIDELINES FOR COMPUTERS, ACADEMY NETWORKS, INTERNET AND VIRTUAL LEARNING ENVIRONMENT USE

General

The students are responsible for good behaviour when using Academy Computers, Academy Networks, Internet and Virtual Learning Environment just as they are in a classroom or an academy corridor. General academy rules apply.

The ICT facilities are provided for students to produce class work, controlled assessment work and homework and to conduct research and where appropriate, communicate with others. Parental permission is required. Remember that access is a privilege, not a right and that access requires responsibility.

Individual users of the ICT facilities are responsible for their behaviour and communications over the network(s). It is presumed that users will comply with academy standards and will honour the agreements they have signed.

Staff may review computer storage areas, files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers or disks would always be private.

During academy, teachers will guide students towards appropriate materials. Students have a responsibility to work within this guidance and report any unsuitable material to their teacher.

The following are not permitted

- Sending, displaying, accessing or trying to access offensive materials
- The use of e-mail systems or access to social networking sites, newsgroups including instant messaging, forums, blogs, wikis and chat rooms, except in specific lessons as directed by a member of staff
- Unsupervised access to the Internet
- Using obscene, threatening or abusive language
- Harassing, insulting or attacking others
- Damaging computers, computer systems or computer networks
- Violating copyright laws
- Using others' passwords or user areas
- Trespassing in others' folders, work or files
- Intentionally wasting limited resources
- Downloading games, using executable programs, running scripts or using unlicensed software
- Disclosing personal details about you or others over the Internet
- Pen Drives or any external storage devices

5 Sanctions

1. Violations of the above rules will result in a temporary or permanent ban on the use of the computers.

2. Additional disciplinary action may be added in line with existing practice.

3. When applicable, police or local authorities may be involved.

INTERNET AND COMPUTER FACILITIES PARENT/CARER PERMISSION FORM

The completed slip should be returned to the academy office.

Name of Student _____ Tutor Group_____

Student

I have read the academy's Acceptable IT Use Policy. As a user of the academy's ICT facilities including the Computers, Networks, the internet and the Virtual Learning Environment, I agree to comply with the academy rules on its use. I will use the network in a responsible way and observe all restrictions explained to me by the academy.

Student Signature _____ Date____/____/____

Parent/Carer

I have read the academy's Acceptable IT Use Policy. As the parent or legal carer of the student signing above, I grant permission for my son/daughter to use the ICT facilities including the Computers, Networks, internet and the Virtual Learning Environment. I understand that students will be held accountable for their own actions. I also understand that some materials on the internet may be objectionable and I accept responsibility for setting standards for my son/daughter to follow when selecting, sharing and exploring information and media.

Parent/Carer Signature _____ Date ____/____/____

LOSTOCK HALL ACADEMY

Acceptable IT Use Policy – Staff

OVERVIEW

The intentions for publishing a Staff ICT Acceptable Use Policy are not to impose restrictions that are contrary to Lostock Hall Academy's established culture of openness, trust and integrity.

Lostock Hall Academy (from here in, known as the Academy) is committed to protecting our Staff, Students and the Academy from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, pen drives, network accounts providing electronic mail, WWW browsing, and File Transfer Protocol, are the property of the Academy.

These systems are to be used only for the purposes of serving the interests of the Academy, and of our students in the course of normal operations.

Effective security is a team effort involving the participation and support of every employee who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment at the Academy. These rules are in place to protect the employee and the Academy. Inappropriate use exposes the Academy to risks including virus attacks, compromise of network systems and services, and legal issues.

SCOPE

This policy applies to employees, contractors, consultants, temporaries, students and other workers at the Academy, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Academy.

POLICY

General Use and Ownership

1. While the Academy's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of the Academy.

Due to the need to protect the Academy's networks, senior management cannot guarantee the confidentiality of information stored on any network device belonging to the Academy.

2. Limited and occasional use of the Academy's systems e.g. Internet access, for personal use is acceptable provided that it is done in a professional and responsible manner, does not otherwise violate the Academy's policy, is not detrimental to the Academy's best interests, and does not interfere with an employee's regular work duties. Employees are responsible for exercising good judgment regarding the reasonableness of personal use and if there is any uncertainty, employees should consult a member of the Senior Leadership Team (SLT).

3. For security and network maintenance purposes, authorised individuals within the Academy may monitor equipment, systems and network traffic at any time.

4. The Academy reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems, including Synergy and
SIMS.Net is classified as confidential, as defined by BECTA confidentiality guidelines, details of which can be found www.becta.org
Employees must take all necessary steps to prevent unauthorised access to the Academy's Networks including prohibiting any students from using all equipment on the Admin Network. This includes ensuring all PC's are either logged off or locked when not in use, or the person is not in the immediate vicinity.
2. Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed every six months.
3. All PCs, laptops and workstations can be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.
4. Use encryption of information in compliance with BECTA guidelines.
5. Postings by employees from their Academy email address should contain a standard Academy signature and disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Academy, unless posting is in the course of business duties.
6. All PC's and Laptops/Notebooks used by the staff and students that are connected to the Academy's Internet/Intranet/Extranet, whether owned or leased by the Academy shall be continually executing an approved virus-scanning software with a current virus database unless overridden by domain group policy.
7. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Unacceptable Use

The following activities are, in general, prohibited, although IT Tech Support Staff may be exempt from these restrictions during the course of their legitimate job responsibilities (e.g., systems/network administration may require them to disable the network access of a host if that host is disrupting services).

Under no circumstances is an employee of the Academy authorised to engage in any activity that is illegal under UK, EU or International law while utilising the Academy's owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited:

1. Violations of the rights of any person or company protected by copyright, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Academy.
2. Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Academy or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, network scanners, unauthorised remote access and phishing tools, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using the Academy's computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment, bullying or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Academy account.
8. Making statements about suppliers, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to the Academy's Tech Support is made in writing.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, the Academy's employees to parties outside the Academy.
16. Failure to secure personal data of students or members of staff in accordance with BECTA's recommended data protection procedures.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, or messaging, whether through language, frequency, or size of messages.
3. Unauthorised use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within the Academy's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the Academy's or connected via the Academy's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Blogging/Posting including all types of digital media on Twitter, Facebook, Instagram etc.

1. Blogging/Posting by employees, whether using the Academy's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy.
Limited and occasional use of the Academy's systems to engage in posting is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the Academy's policy, is not detrimental to the Academy's best interests, and does not interfere with an employee's regular work duties. Blogging/Posting from the Academy's systems is also subject to monitoring.

2. Blogging/Posting should not include any of the Academy's confidential information. As such, employees are prohibited from revealing any of the Academy's confidential or proprietary information, student information or any other material covered by the Academy's Confidential Information policy when engaged in blogging /posting /uploading images.

3. Employees shall not engage in any blogging/posting /uploading images or text that may harm or tarnish the image, reputation and/or goodwill of the Academy and/or any of its employees. Employees are also prohibited from making any discriminatory, racial, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by the Academy's Staff Handbook.

4. Employees may also not attribute personal statements, opinions or beliefs to the Academy's when engaged in blogging/posting /uploading images. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the Academy. Employees assume any and all risk associated with blogging / posting /uploading images.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, the Academy's trademarks, logos and any other of the Academy's intellectual property may also not be used in connection with any blogging/posting /uploading images.

6. Staff should adhere to the 'Guidance on the use of Social Networking sites and other forms of Social Media' issued by Lancashire County Council to be found on the Staff Intranet section of Synergy. Specific rules are detailed below but the policy should be read in its entirety prior to signing the Staff ICT AUP.

Employees who choose to make use of social networking site/media should be advised as follows:

- That employees familiarise themselves with the sites 'privacy settings' in order to ensure that information is not automatically shared with a wider audience than intended.

- That employees do not conduct or portray themselves in a manner which may:

    - bring the Academy into disrepute;
    - lead to valid parental complaints;

- be deemed as derogatory towards the Academy and/or its employees;
- be deemed as derogatory towards students and/or parents and carers;
- bring into question their appropriateness to work with children and young people.

- That employees do not form on-line 'friendships' or enter into communication with *parents/carers and students as this could lead to professional relationships being compromised.

- On-line friendships and communication with former students should be strongly discouraged particularly if the students are under the age of 18 years.

(*In some cases employees in Academy's/services are related to parents/carers and/or students or may have formed on-line friendships with them prior to them becoming parents/carers and/or students of the Academy/service. In these cases, employees should be advised that the nature of such relationships has changed and that they need to be aware of the risks of continuing with this method of contact. They should be advised that such contact is contradictory to the Specific Guidance points above.)

7. Staff should adhere to the DfE document 'Guidance for Safer Working Practices for Adults Working with Children and Young People in Educational Settings issued 2020, which states:

Communicating with both current and former students via social networking sites or via other non-Academy related mechanisms such as personal e-mails and text messaging can lead to employees being vulnerable to serious allegations concerning the safeguarding of children and young people.
Communication between students and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.

Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to students including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. E-mail or text communications between an adult and a child young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites. *(Lostock Hall Academy employees should not give out their personal contact details, but instead should use official Academy channels, including the Academy mobile phone).*
Internal e-mail systems should only be used in accordance with the Academy/service's policy.

Internet Filtering – All Networks
Online Safety Internet Filtering

It is the duty of care for all LHA Staff to be vigilant and monitor student activities especially when actively using the internet.
Due to the responsibilities and accountabilities in the Academy's Internet Filtering/Online Safety policies, Board of Trustees, SLT and Staff could be held personally liable if they operate outside the relevant policies.
Should any potentially inappropriate content be noticed, on any of the academy networks, it is the responsibility of the staff member who either discovers them, or is informed of this by students, to follow the following guidelines.

Web Filtering Incident Procedure

1) Briefly investigate the content of the incident to verify, and if you have any concerns report and gather information.
2) Capture and preserve as much relevant information as possible as this may be required later in the form of evidence – possibly submitted to other external agencies.
3) Report the incident immediately to the Academy's Online Safety Coordinator and notify your Line Manager/SLT/Principal as appropriate.
4) Log a call online via the correct Online Safety category in Synergy/Sysaid to time and date stamp the incident and also to record the exact details of what happened along with any other information e.g. screenshots, URLs etc.

YouTube/Streaming

Staff need to be fully aware that the likes of YouTube, Vimeo, etc., can, and often do return adult/sexual/racial content when browsing these and many other internet sites. This can be in the form of images or user comments.

If live internet content is to be displayed within a public or classroom environment, it is the employee's responsibility to ensure that any inappropriate content is not relayed to others via any projectors/screens which may be connected to the employee's laptop/PC.

All Staff should therefore use the screen blanking facility on projectors to avoid any inappropriate content accidently being displayed.

ICT CODE OF CONDUCT – WITHIN AND OUTSIDE ACADEMY

In agreeing to this code of conduct agree to follow the guidance in the Policy as a whole as well as the specific areas below:

- I will ensure that my ICT use will always be compatible with my professional role and in accordance with Lostock Hall Academy's Acceptable Use Policy.
- I understand that the Academy may monitor my ICT use as part of its duty of care to all members of the Academy community.
- I will respect system security and I will not disclose any password or security information to anyone. If it is suspected that a password has been compromised I understand that it must be changed immediately.
- I will not leave a work station unattended when I am logged in, instead I will lock the computer.
- I will not store confidential material on network areas which are accessible to persons who do not have clearance to access such material.
- I take full responsibility for the security/appropriate use of any Academy ICT which I use away from Academy premises. I recognise that any discovery of inappropriate and/or offensive material will be fully investigated and will lead to disciplinary action.
- I will write any messages carefully and politely, particularly as email could be forwarded to unintended readers. I understand that any anonymous messages and chain letters are not permitted.
- I will ensure that personal data is kept secure, by using encryption, and is used appropriately, whether in Academy, taken off the premises or accessed remotely.
- I understand that I should use Academy ICT to deal with Academy business and not use my own personal ICT e.g. personal contact details such as mobile phone number and email address.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern to an appropriate member of the Academy's SLT.
- I will ensure that any ICT communications with students are compatible with my professional role.
- I will promote online safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I understand that use of any Academy ICT for personal financial gain, gambling, political purposes or advertising is forbidden. Use of Academy ICT to access inappropriate materials such as pornography or incitement sites (seeking to incite racism, homophobia, self-harm, suicide etc.) or other offensive material is forbidden.

- I understand this policy may be subject to alteration at any time in order to meet any changed requirement in law of DfE guidance.

ENFORCEMENT

The Academy will exercise its right to monitor the use of the Academy's ICT, including Internet access, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the Academy's information system or resources may be taking place, or the system being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

DEFINITIONS/GLOSSARY

Denial-of-service attack (**DoS attack**) or **distributed denial-of-service attack** (**DDoS attack**) is an attempt to make a computer or network resources unavailable to its intended users to prevent an Internet site or a network service from functioning efficiently or at all, temporarily or indefinitely. Such attacks usually lead to a server or network overload.

E-mail bomb - In Internet usage, an **email bomb** is a form of net abuse consisting of sending huge volumes of email to an address in an attempt to overflow the mailbox *or* overwhelm the server where the email address is hosted.

Email spoofing is email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a different source. The result is that, although the email appears to come from the address indicated in the *From* field, it actually comes from another source.

Encryption - is the process of translating data into a secret code to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

File Transfer Protocol (**FTP**) is a standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet.

Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication such as from popular social web sites, banks and auction sites. Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

Port scanner is a software application designed to probe a server or host for open ports which if successful could access the network illegally.

Port sweep is to scan multiple PC's or Servers for a specific port, in order to access the network illegally.

Pyramid scheme is a non-sustainable business model that involves promising participants' payment or services, primarily for enrolling other people into the scheme, rather than supplying any real investment or sale of products or services to the public.

Spam - The sending of unsolicited or unauthorised e-mails.

Trojan horse, or **Trojan**, is software that appears to be legitimate but performs a harmful activity when it runs such as stealing information or causing damage.

(Computer) Worm is a self-replicating malware computer program, which uses a computer network to send copies of itself to other computers and it may do so without any user intervention. Unlike a computer virus, it does not need to attach itself to an existing program.

INTERNET AND COMPUTER FACILITIES STAFF AGREEMENT

By signing below, I agree that I have read, understand and agree to the terms and conditions of the Academy's Staff ICT Acceptable Use Policy and the 'Guidance on the use of Social Networking sites and other forms of Social Media.

Print Name _____

Signature _____

Date _____