E SAFETY POLICY
Statement of Practice

LEES BROOK COMMUNITY SCHOOL

Document Owner	Catherine Heffern Deputy Head
Date Reviewed	1 February 2021

Introduction

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

The purpose of this policy is twofold:

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

It is important to teach students about the underpinning knowledge and behaviours that can help them navigate the online world safely and confidently regardless of the device, platform or app. We want to equip our students with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way so that they are able to reap the benefits of the online world.

Related Policies, Statements of Practice and procedures

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

- Behaviour Policy
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Student IT Code of Conduct and Parental consent for Internet access (Appendix 1)
- Staff IT Security and Usage Policy (Appendix 2)
- E-Safety Policy (Remote Education) Covid 19 Addendum

Statement of Practice
E Safety Policy

Governing Body

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

- Review this policy at least annually and in response to any Online Safety incident to ensure that the policy is up to date and covers all aspects of technology use within the school;
- Ensure online-safety incidents are appropriately dealt with and that the policy was effective in managing those incidents;
- Appoint a governor with responsibility for Safeguarding, including Online safety who will:

    - Keep up to date with emerging risks and threats through technology use;
    - Receive regular updates from the Headteacher with regards to training, identified risks and any incidents.

Headteacher

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

The Headteacher will ensure that:

- Online Safety training throughout the school is planned, up to date, appropriate to the recipient, i.e. students, all staff, leadership team, governing body and parents;
- All Online Safety incidents are dealt with promptly and appropriately through the 'MyConcern' and Class Charts reporting systems.

Online Safety Officer

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

- Keeping up to date with the latest risks to children whilst using technology; familiarising themselves with the latest research and available resources for school and home use;
- Reviewing this policy regularly and bringing any matters to the attention of the Headteacher;
- Advising the Headteacher and governing body on all Online Safety matters;
- Advice on engaging parents and the wider school community on Online Safety matters at school and/or at home;
- Monitoring 'MyConcern' and Class Charts and ensuring an appropriate audit trail

In conjunction with IT support:

- Liaising with the local authority, IT technical support and other agencies as required;
- Ensuring any technical Online Safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose.
- Making themselves aware of any reporting function with technical Online Safety measures, i.e. internet filtering reporting function and liaising with the Headteacher and responsible governor to decide on what may be appropriate for viewing.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood, it should be brought to the attention of the Headteacher as soon as practically possible.
- Any Online Safety incident is reported through the use of 'MyConcern' and Class Charts. If uncertainty exists as to whether an incident involves Online Safety, staff should raise the issue with the Online Safety Officer or the Headteacher and defer to them.

All Students

The boundaries of use of ICT equipment and services in the school are given in the Student ICT Code of Conduct

Online Safety is embedded across the ICT and Citizenship curriculum and students will be given the appropriate advice and guidance by staff. Messages about Online Safety will be reinforced in assembly and tutor activities. The misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

Parents and Carers

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

Technology

Lees Brook uses a range of devices, including PCs and chrome books to support the day-to-day operation of the school and the education of all students. Year 11 students may also use their own mobile devices during designated Form Tutor sessions to assist in exam preparation. In order to safeguard the student and in order to prevent loss of personal data, we employ the following technology or policies:

Computer Usage Monitoring /Classroom Management — We use Impero Software for the monitoring and logging of all activity by users in the school. It uses policies, word lists and website lists to detect and log (via screenshot, website/window history etc.) any student viewing unsuitable content, accessing indecent images, cyberbullying, grooming, identity theft, radicalisation and terrorism.

Teaching staff should pass on any screenshots/concerns they have about what a student has been accessing/viewing to the IT Systems team who can then check the full logs/update the Internet filter etc.

Internet Filtering/Firewall — We use Sophos Unified Threat Management. The Sophos Web Protection filter prevents malware infections, spyware and viruses from entering the network via the internet.

All website access is logged against each user across both the school network and any connected personal device.

All Internet filtering is reviewed in line with this policy or in response to an incident, whichever is sooner. The IT Systems Team are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering — We use Microsoft Office 365 for our e-mail solution along with its built in spam and anti-malware filters that prevents any infected email from being sent or received by users in the school.

Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data and spam email such as a "phishing" message intended to trick the recipient into handing over their personal data or login details for public (usually financial) websites.

Encryption and Data Protection — All school devices are configured to automatically store information — personal (as defined by the Data Protection Act 1998) or otherwise — on the central server, where it is secured

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

Passwords — all staff and students need a unique username and password to access the computing facilities. The computer systems are configured to force users to choose “secure” passwords (a minimum of 8 characters featuring at least 3 of the following: uppercase letter, lowercase letter, number and an extended character). Staff and student passwords will be changed if there is a compromise. The IT Systems Team are responsible for ensuring that passwords are changed when needed.

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

Lees Brook accepts no liability for any loss or damage to students own mobile devices.

Safe Use

Internet, e-mail and software use in school

- Students and Parents must read and sign the Code of Conduct. They must agree to the school viewing, with just reason and without notice, any emails they send or receive, material they store on the school’s computers, or logs of websites they have visited.
- School computer and Internet use must be appropriate to student educational activity. Students must only access those services they have been given permission to use and they must not access the internet or e-mail for inappropriate purposes. The work/activity on the Internet and e-mail must be directly related to the student’s school work and they must not give their password or log-in name to anyone.
- When working on a school PC or chromebook students must take care to “Lock” the device should they have reason to be away from their screen. This is to prevent other students from being able to access software and emails. If a student suspects that their account has been accessed by another student they should report this to a teacher immediately.
- Students must not give personal information to anyone on the internet or by e-mail and they must not view, upload or download, or send by email, any material which may infringe copyright or is likely to be unsuitable for children or the school. This applies to any material of a violent, dangerous or racist nature or containing inappropriate sexual content. If they are unsure, they must ask a teacher for clarification.
- Students must be polite and appreciate that other users might have different views than their own. The use of strong language, abusive language or aggressive behaviour is not allowed. Students must not write anything on a website or send by e-mail anything which could be offensive. They must not use the internet in or out of school to bully, threaten or abuse other students and they must not use the internet in or out of school for any purpose that may bring the school into disrepute.

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

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

Staff Email Usage

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

Social Networking and Online Bullying

- The term 'social networking' refers to any website or digital resource designed to facilitate social interaction between people in either private or public online spaces.
- Online bullying, e-bullying or cyber bullying, is defined as follows: 'the use of information and communication technologies such as email, [mobile] phone and text messages, instant messaging, defamatory personal websites and defamatory personal polling websites, to support deliberate, repeated, and hostile behaviour by an individual or a group, that is intended to harm others.'
- If a student is being bullied online, he/she should immediately seek help from a teacher, parent or carer. They should not respond to the messages, but should keep a detailed diary recording information such as the content of the message, the date, the time, the caller ID, username, or email address, and whether the number was withheld or not available. If space permits, the messages should also be stored on the phone, or in the email account, in case they are needed later as evidence.
- Online bullying is considered as serious as any other form of bullying, and similar sanctions will be applied, as outlined in our Anti Bullying Policy.
- Failure to comply with these rules will result in a ban, temporary or permanent, on the use of the Internet facilities at school and a letter informing their parents of the nature and breach of the rules. Appropriate sanctions and restrictions placed on access to school facilities may result and temporary or permanent exclusion for abuse of the school's ICT facilities and of the internet may be used in extreme or persistent cases.

Text Messaging/Mobile Phones

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

Students are allowed to bring mobile devices into school. However, these should be switched off as they enter school and placed in the bottom of their school bag.

Curriculum

Students will be taught about online safety and harms through subjects such as Relationships and Sex Education. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their student's lives.

This will complement the Computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content on the internet or other online technologies.

There are also other curriculum subjects which include content relevant to teaching students how to use the internet safely. For example Citizenship and Media Studies cover media literacy – distinguishing fact from opinion as well as exploring freedom of speech and the role and responsibility of the media in informing and shaping public opinion. It also supports teaching about the concept of democracy, freedom, rights and responsibilities.

Key Personnel:

Headteacher – Zoe House
DSL – Sarah Hadwin
Online Safety Officer – Catherine Heffern
Safeguarding Governor – Mike Ainsley

Student ICT Code of Conduct Appendix 1

Student ICT Code of Conduct

Use of computers:

I will:

- Only enter an ICT suite or use a classroom computer with permission from a member of staff
- Use all equipment sensibly
- Not eat food or drink whilst in an ICT suite or using a computer without the permission of the teacher
- Not attempt to move or unplug any of the equipment without instruction from a member of staff
- Treat the equipment with respect
- Not attempt to install, change or remove software
- Only use the computer network to complete appropriate work and help support my education and research

Network security:

I will:

- Only access the computer network using my own authorised username and password
- Not tell anyone my username and password as I understand I am responsible for anything that is done on a computer in my username and I will face the consequences of it
- Not attempt to log on to another student's computer area or tamper with their work when they are logged on
- Tell a member of staff if I think another student has been logging in to my user account
- Not attempt to breach the school's network security systems

Keeping myself safe:

I will:

- Not use the school computer facilities or my mobile phone to send bullying messages or upset others
- Not give my home address or phone number to anyone online or arrange to see someone via the internet
- Help to protect myself and other students by reporting anything I see on a computer or mobile phone that I am unhappy with
- Not search the internet for, or send/receive emails or other messages that contain pornographic, unethical or illegal requests, or any other inappropriate use which is likely to cause offence
- Not attempt to use public chat rooms during the school day

Monitoring:

I understand that the school will exercise its right to monitor the use of the school computer systems including:

- Websites
- Printer usage
- Interception of emails
- The deletion of inappropriate materials
- The storing of text imagery or multimedia files which are unauthorised or unlawful

Remote Learning:

In addition to following all of the rules listed, when working remotely I will:

- Complete work to any deadline that is set by teachers
- Seek help if I need it, from teachers
- Alert teachers if I am not able to complete work that has been set
- Use proper online conduct, such as using appropriate language in messages

Agreement:

I have discussed the code with my parent/carer and agree to follow the online safety rules and to support the safe and secure use of ICT at Lees Brook Community School.

Student name _____ Signature _____ Date _____

Parent/Carer Name _____ Signature _____ Date _____

Staff ICT Security and Usage policy Appendix 2

Staff must not use, or try to use the IT facilities at Lees Brook Community School – including the email or internet facilities – to create, distribute or display in any form, any activity that is or may be considered to be against the law, against school policies or that may lead to a legal claim being made against the school.

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

- Pornographic or obscene;
- Intimidating, discriminatory (for example; racist, sexist or homophobic);
- Defamatory;
- Hateful or encouraging violence or strong feelings;
- Fraudulent or showing or encouraging criminal acts;
- Unethical or may bring the school into disrepute or
- A deliberate harmful attack on systems used, owned or otherwise run by the school.

The school will only allow staff to access such material, with written confirmation, if it is necessary as part of an investigation or to ensure the safety of young people in the school's care. Should staff inadvertently access such material, they must report the incident to the Online Safety Officer immediately. If staff find or suspect anyone of using the computer system illegally or unethically, they must report it to the Online Safety Officer immediately who will advise the Headteacher.

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

Confidential or sensitive information

By using the school's ICT facilities, staff may become party to sensitive or confidential information relating to young or vulnerable people, or confidential information relating to the day-to-day business operations of the school. Personally identifiable or other personal information relating to students and other members of staff is governed by GDPR and staff must not breach these regulations.

USB data devices are insecure and easily stolen or lost and staff are advised not to store confidential or sensitive information on a USB memory device unless the device itself has been encrypted. Disciplinary or legal action may be brought against a member of staff who knowingly stores confidential or sensitive information related to the school, students or members of staff in an insecure manner on such a device and then loses it.

Access to Email and Internet Services

The school email and internet facilities are for business use but Lees Brook Community School will allow staff to use them privately as long as it is reasonable ie quickly checking the weather, a transport timetable or reading the news during a break. Conversely, 'unreasonable' use may be considered as any private internet or email use that is allowed to be a distraction to the role, is classed as a data or child protection issue, contravenes copyright legislation or threatens the security of the network in any way.

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

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

Use of social networking Internet sites

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

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

It is recommended that staff using social networking sites should:

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

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

Email good practice

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

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

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

Passwords

The only person staff should ever release their password to, if expected to do so, is the Headteacher. Staff are instructed not to tell anyone else their password without the Headteacher's explicit confirmation, even if requested over the telephone, no matter how genuine the caller or reason may seem. The only person who can request that the password of a staff member can be changed in their absence is the Headteacher.

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

Staff need a unique username and password to access the computing facilities. The computer systems are configured to force users to choose "secure" passwords (a minimum of 8 characters featuring at least 3 of the following: uppercase letter, lowercase letter, number and an extended character). Chosen passwords should not be obvious or 'guessable' e.g. surname, date of birth, pet or children's names and staff are encouraged to change their passwords on a regular basis. Staff and student passwords will be changed if there is a compromise. The IT Systems Team are responsible for ensuring that passwords are changed when needed.

It is strongly advised that staff never write passwords down although in certain circumstances recording a password may be acceptable providing it is stored securely i.e. for disaster recovery purposes. If a member of staff suspects that someone else knows their password, they must change it immediately.

Computer viruses

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

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

If a virus is found, or suspected, staff are instructed to immediately stop using the computer and request advice from the Network Manager. Staff must always follow the instructions that the Network Manager gives in relation to virus attacks or other security issues. Virus warnings from any other source other than the Network Manager must only be forwarded onto the Network Manager who will then confirm its validity and decide on the next course of action.

Recording Usage

Staff should be aware that use of Lees Brook's facilities is audited to help the school ensure that the integrity of the system is maintained. This includes the recording of all internet sites accesses and the monitoring of email. This is covered under the Telecommunications (lawful Business practice) (Interception of Communications) Regulations 2000.

If staff inadvertently access an internet site containing prohibited material, they must break the connection immediately and report it to the Network Manager.

Copyright

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

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

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

Software is also protected by copyright and must not be installed by staff themselves. This includes seemingly innocuous 'free' software from the Internet. By doing so, staff may be in violation of a license agreement or be introducing 'Trojan horse' software that could damage the integrity of the network or files. All software must be used strictly in accordance with the terms of its license.

Agreement

By confirming that you have read and understood this policy on ''MyConcern', you agree to follow this security and usage policy and to support the safe and secure use of ICT throughout Lees Brook Community School.