E SAFETY POLICY

Date Drafted:	**May 2019**
Date Adopted by LGB:	**June 2019**
Review Frequency:	**Annually**
To be Reviewed By:	**Director of Safeguarding (DSL)**

Merrill Academy is committed to:
•Raising standards of achievement and creating opportunities for all pupils, regardless of needs to develop their full potential and improve their life chances.
•Raising the aspirations of the whole school community by creating a culture of continuous learning that celebrates success at all levels.
•Developing a school that is the pride of the local area where pupils, parents, staff, governors and wider community feel valued, listened to and welcomed for the diverse contribution they make to our school life.

E-Safety Policy

Link with other policies:
• ICT Acceptable Use Security Policy
• ICT Agreement – Student and School
• Child Protection and Safeguarding Policy
• Anti-Bullying

Why our school needs an E-Safety Policy

The Governing Body at Merrill Academy believes that the use of information and communication technologies in school brings great benefits. Recognising the E-Safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications. In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger. We are aware that young people can be exposed to extremist influences or prejudiced views from an early age which emanate from a variety of sources including via the internet.

E-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of School. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

The right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. School is aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good E-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to understand about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.
Breaches of an E-Safety policy can and have led to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider School community. It is crucial that all individuals are aware of the offline consequences that online actions can have.
The school have legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit with the Head Teacher and the Governing Body.

The E-Safety policy is essential in setting out how the School plans to develop and establish its E-Safety approach and to identify core principles which all members of the School community need to be aware of and understand.
Teaching and Learning
• The school Internet access is designed for student use and includes filtering appropriate to the age of students.
• Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
• Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
• The school will ensure that the use of Internet derived materials by staff and students complies with copyright law.
• Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

• Information system security School ICT systems capacity and security will be reviewed regularly.
• Virus protection is robust will be updated regularly.
• Staff will be alert to pupils accessing extremist material online, including through social networking sites.
Management of E-mails account:
• Students may only use approved e-mail accounts on the school system.
• Students must immediately tell a teacher if they receive offensive e-mail.
• School reserve the right to monitor emails for the safety of students and staff, under the current human rights legislation.
• It is important that staff should use a work provided email account to communicate with parents/carers, pupils and other professionals for any official School business. This is important for confidentiality and security and also to safeguard members of staff from allegations.
• Email accounts should not be provided which can be used to identify both a student's full name and their School. Spam, phishing and virus attachments can make email dangerous.
• Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
• Access in School to external personal email accounts may be blocked.
• Excessive social email use can interfere with learning and will be restricted.
• Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on School headed paper would be.
• The forwarding of chain messages is not permitted.

• School will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
• Staff should not use personal email accounts during School hours or for professional purposes.

Published content and the school web site:
• The School website complies with the School 's guidelines for publications including publication of the required policies and privacy statements and respect for intellectual property rights and copyright.
• The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
• The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing student's images and work:

Small images of groups of students should be used and where possible using images that do not show faces at all. Personal photographs can be replaced with self-portraits or images of students' work or of a team activity. Students in photographs should, of course, be appropriately clothed.
• Written consent will be kept by the School where pupils' images are used for publicity purposes, until the image is no longer in use.
• Student's work can only be published with the permission of the student and parents.
• Images or videos that include students will be selected carefully and will not provide material that could be reused.
• Students' full names will not be used anywhere on the website, particularly in association with photographs.

Social networking and personal publishing:

• The school will block/filter access to social networking sites.
• Newsgroups will be blocked unless a specific use is approved.
• Students will be advised never to give out personal details of any kind which may identify them or their location.
• Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff must obtain documented consent from the Head Teacher before using Social Media tools in the classroom.
• Staff official blogs should be password protected and run from the School website with approval from the Head Teacher. Members of staff must not run social network spaces for pupil use on a personal basis.
• All members of the School community are not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
• Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the School ICT Acceptable use and Security Policy.

Managing filtering:

• The school will work with the Local Authority and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
• If staff or pupils discover an unsuitable site, it must be reported to the IT Technicians.
• SLT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Emerging Technologies:

• Mobile phones should not be used during formal school time.
• I watches or any other wearable web enabled device is not allowed
• The sending of abusive or inappropriate text messages is forbidden.
• Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

How will information systems security be maintained?

The ICT Support Team in school are aware of security issues of Local Area Network (LAN) to include:
♣ Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
♣ Users must take responsibility for their network use.
♣ Workstations will be secured against user mistakes and deliberate actions.
♣ Server is located securely and physical access restricted.
♣ The server operating system is secured and kept up to date.
♣ Virus protection for the whole network must be installed with the latest version.
♣ Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.
.
The School Broadband network is protected by a cluster of high performance firewalls. These industry leading appliances are monitored and maintained by a specialist company.
● The security of the School Management Information Systems (MIS) and users will be reviewed regularly.
● Virus protection will be updated regularly.
● Personal data sent over the Internet or taken off site will be encrypted.
● Portable media may not be used without specific permission followed by an anti-virus / malware scan.
● Unapproved software will not be allowed in work areas or attached to email.
● Files held on the School's network will be regularly checked and cleared twice a year.
● The ICT Support team will review system capacity regularly.
● The use of user logins and passwords to access the School network is enforced.

Protecting personal data:

Personal data will only be recorded, processed, transferred and made available according to the GDPR Policy.

How will Cyberbullying be managed?
Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone".

There are a number of statutory obligations on School with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006:

♣ Every School must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the School 's behaviour policy which must be communicated to all pupils, School staff and parents

♣ Gives Head teachers the ability to ensure that pupils behave when they are not on School premises or under the lawful control of School staff.

Bullying outside School (such as online or via text) reported to the School will be investigated and acted on.

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If School staff feel that an offence may have been committed they should seek assistance from the police.

For more information please read "Preventing and Tackling Bullying: Advice for School Leaders, Staff and Governing Bodies"
http://www.education.gov.uk/aboutdfe/advice/f0076899/preventing-and-tackling-bullying
DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying:
http://www.digizen.org/cyberbullying

• Cyberbullying (along with all other forms of bullying) of any member of the School community will not be tolerated.
• There are clear procedures in place to support anyone in the School community affected by cyberbullying.
• All incidents of cyberbullying reported to the School will be recorded.
• Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.
• The School will take steps to identify the bully, where possible and appropriate. This may include examining School ICT system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
• Students, staff and parents/carers will be required to work with the School to support the approach to cyberbullying and the School's E-Safety ethos.
• Sanctions for those involved in cyberbullying may include:
- Asking the bully to remove any material deemed to be inappropriate
- a service provider may be contacted to remove content if the bully refuses or is unable to delete content
- Internet access may be suspended at School for the user for a period of time.
- Other sanctions for pupils and staff may also be used in accordance to the School anti-bullying, behaviour policy or ICT Acceptable Use Policy.
- Parent/carers of pupils will be informed.

The Police will be contacted if a criminal offence is suspected.