Bishop Stopford School

faith | justice | responsibility | truth | compassion

e-Safety Policy

Review Date : April 2020

Review by : Personnel/Student Care and Discipline Committee

School Context

The Core Values which relate specifically to this policy state that we are working together to form relationships based on

- **Justice** – everyone in school is entitled to be treated fairly and to promote the self-esteem of others.
- **Responsibility** – everyone in school is expected to understand the consequences of their actions.
- **Truth** – everyone in school is required to be honest and to communicate in a positive manner.

Such values contribute to our common purpose of “Striving for high quality education with a strong Christian ethos”, and as such underpin e- e-safety procedures within the Academy.

Data Protection

- Any personal data processed in the delivery of this policy will be processed in accordance with the school Data Protection policy.

Context:

ICT and the Internet have become integral to teaching and learning within schools, providing students and staff with opportunities to improve understanding, access online resources and communicate with the world all at the touch of a button. At present, the Internet based technologies used extensively by young people in both home and school environments include:

- Websites
- Social Media, including Facebook and Twitter
- Web enabled mobile/smart phones/smart watches
- Online gaming
- Learning Platforms and Virtual Learning Environments
- Video broadcasting,
- Blogs and Wikis
- Email, Instant Messaging and Chat Rooms

Whilst this technology has many benefits, clear procedures for appropriate use and education for staff and students about online behaviours, age restrictions and potential risks is crucial.

All schools have a duty to ensure that students are protected from potential harm both within and beyond the school environment. Every effort will be made to safeguard against risks.. Any incidents that do arise will be dealt with quickly and according to policy to ensure that students and staff continue to be protected.

Aims

- To emphasise the need to educate staff and students about the pros and cons of using new technologies both within, and outside of, the school environment.
- To provide safeguards and rules for acceptable use to guide all users in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school or educational setting.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

Scope of the Policy

This policy applies to all staff, students, governors, visitors and contractors accessing the internet or using technological devices on school premises. This includes staff or students use of personal devices, such as mobile phones or other mobile devices which are brought onto school grounds. This policy is also applicable where staff or individuals have been provided with school issued devices for use off-site, such as school laptop or work mobile phone.

Staff Responsibilities

Teaching and Support Staff (including volunteers)

All staff have a shared responsibility to ensure that students are able to use the Internet and related technologies appropriately and safely as part of the wider duty of care to which all who work in schools are bound.

The Acceptable Use Policy outlines further details regarding staff responsibilities and expectations for behaviour whilst accessing the internet, email or related technologies within and beyond school. This document is made available to all staff and shared with any volunteers, visitors or contractors when they log on to the school network.

Network Manager

The Network Manager is responsible for ensuring:

- that the school's ICT infrastructure is secure and not open to misuse or malicious attack
- that anti-virus software is installed and maintained on all school machines and portable devices
- that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the E Safety Lead and the Designated Person for Safeguarding
- that any problems or faults relating to filtering are reported to Designated Person for Safeguarding and to the broadband provider immediately and recorded on the e Safety Incident Log
- that users may only access the school's network through a rigorously enforced password protection policy, in which passwords are regularly changed
- that he/she keeps up to date with e safety technical information in order to maintain the security of the school network and safeguard students
- that the use of the school network is regularly monitored in order that any deliberate or accidental misuse can be reported to the E Safety Lead.

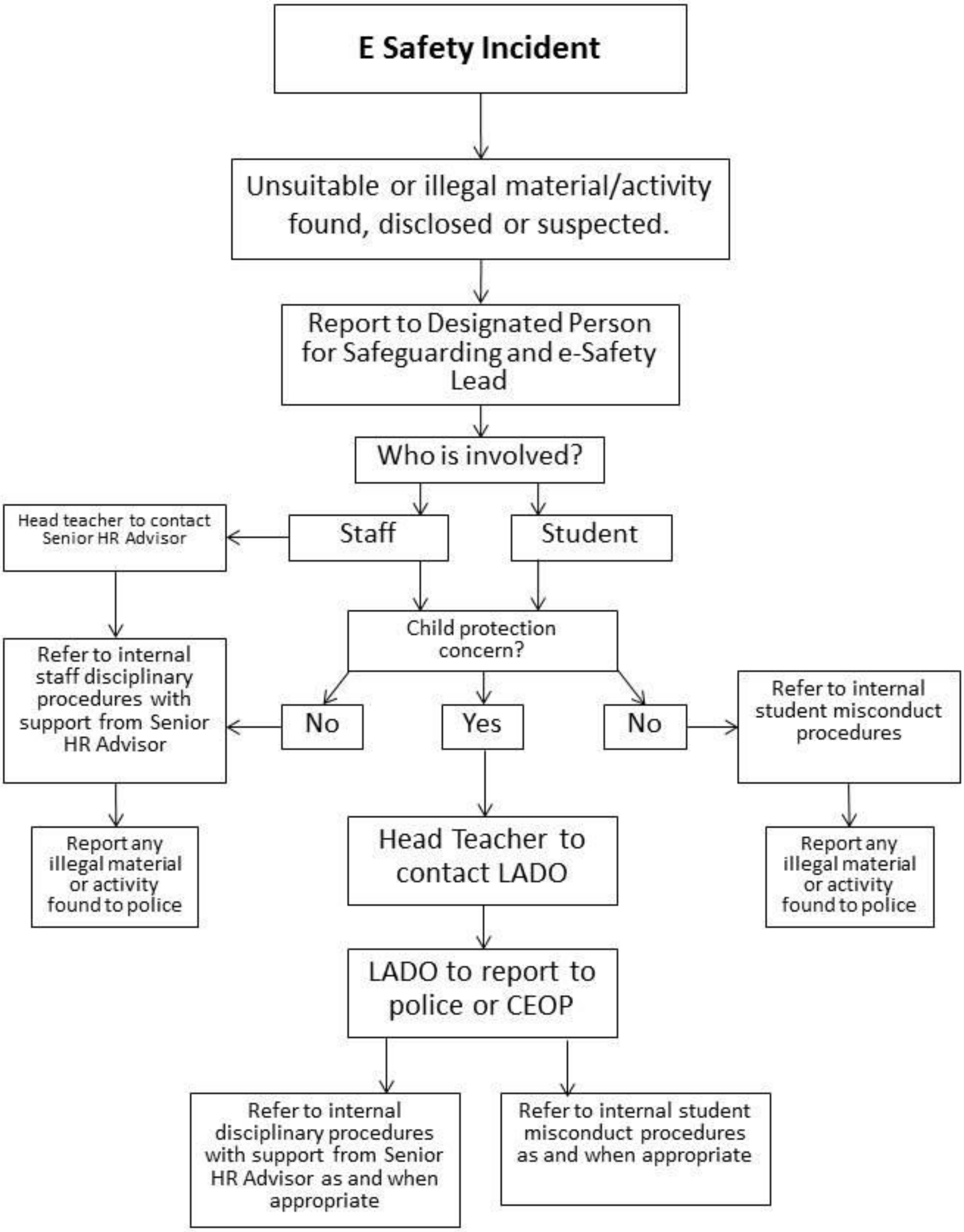
Students

Students are responsible for:

- Complying with the Acceptable Use policy when using the Academy's network
- Using the Internet and technologies in a safe and responsible manner within school.
- Informing staff of any inappropriate materials, cyberbullying or contact from unknown sources (age dependant)
- Actively participating in the review of the Acceptable Use rules.

Incident Reporting

In the event of misuse by staff or students, including use of the school network in an illegal, unsuitable or abusive manner, a report must be made to the Head teacher/Designated Person for Safeguarding immediately and the e Safety Incident Flowchart followed.


E Safety Incident
Unsuitable or illegal material/activity found, disclosed or suspected.
Report to Designated Person for Safeguarding and e-Safety Lead
Who is involved?
Staff
Student
Head teacher to contact Senior HR Advisor
Child protection concern?
No
Yes
No
Refer to internal staff disciplinary procedures with support from Senior HR Advisor
Refer to internal student misconduct procedures
Head Teacher to contact LADO
Report any illegal material or activity found to police
Report any illegal material or activity found to police
LADO to report to police or CEOP
Refer to internal disciplinary procedures with support from Senior HR Advisor as and when appropriate
Refer to internal student misconduct procedures as and when appropriate

In the event of minor or accidental misuse, internal investigations should be initiated and disciplinary procedures followed where appropriate. Additionally, all security breaches, lost/stolen equipment or data, unauthorised use or suspected misuse of ICT should be reported immediately to the Head Teacher, Network Manager and Senior Information Risk Owner (SIRO).

All incidents must be recorded by student services to allow for monitoring, auditing and identification of specific concerns or trends.

Monitoring

School ICT technical staff regularly monitor and record user activity, including any personal use of the school ICT system (both within and outside of the school environment) and users are made aware of this in the Acceptable Use Policy. Monitoring of the school network is carried out using the school's web filter and a report produced every month. Web filter reports are analysed and monitored by the e-safety team. Networked computers are also routinely monitored using Impero software.

The Curriculum

The school strives to embed e Safety in relevant areas of the curriculum.

- Skills and competencies are taught across KS3 to ensure that students are able to explore how online technologies can be used effectively, but in a safe and responsible manner.
- GCSE students are made aware of copyright issues, data protection, intellectual property and reliability of information sourced on the internet as part of the ICT curriculum.
- Opportunities for discussions in PSHE about online risks and strategies for online protection are built into the curriculum, Students, parents and staff are signposted to national and local organisations for further support and advice relating to e safety issues, including Cybermentors, BeatBullying, Childline, EducateAgainstHate and CEOP.

Email Use

Staff

- The school provides all staff with a professional email account to use for all school related business, including communications with children, parents and carers. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.
- Under no circumstances will staff members engage in any personal communications with current students outside of authorised school systems.
- Protocols for acceptable use of email are outlined in the Academy's Email Etiquette document
- Staff should inform the e Safety Lead if they receive an offensive or inappropriate email via the school system.

Students

- The Academy provides individual email accounts for students to use as part of their entitlement to understand different ways of communicating and using ICT to share and present information.
- Students will use their school issued email account for any school related communications, including homework or correspondence with teachers. Email content will be subject to monitoring and filtering for safeguarding purposes.
- The forwarding of chain letters is strictly prohibited in school and should be reported to a member of staff immediately.

Both

- It is the responsibility of each account holder to keep their password secure and to report any suspected breaches of password security to the Network Manager. Account holders must never share their password with another user, or allow access to their email account without the express permission of the Head Teacher.

Managing remote access

As technology continues to develop at an exponential rate, schools and their staff are increasingly taking advantage of opportunities for off-site access to the school network and email using remote access facilities. For data security and safeguarding purposes, it is crucial that staff are aware of the following restrictions on use:

- Only equipment with the appropriate level of security should be using for remote access (i.e. encryption on any devices where sensitive data is stored or accessed)
- Log-on IDs and PINs should be confidential and use information that cannot be easily guessed (e.g. date of birth, telephone number, number patterns)
- For security purposes, network access information should not be written down or stored with the device in case of theft or unauthorised access.

Internet Access and Age Appropriate Filtering

Broadband Provider: Virgin Media
Web filtering Provider: Cisco Meraki

All students are entitled to safe and secure Internet access and schools have a duty to deliver this as part of the learning experience. The Head teacher is ultimately responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that age appropriate internet filtering is in place to protect young users from inappropriate or harmful online content. To this end, the school has the following filtering measures in place:

- Filtering levels are managed and monitored in school via an administration tool/control panel, provided by our web filtering supplier, which allows an authorised staff member to instantly allow or block access to a site or specific pages and manage user Internet access.
- Filtering levels are managed and monitored on behalf of the school by our broadband and web filtering supplier, allowing an authorised school staff member to allow or block access to site and manage user internet access.
- Age appropriate content filtering is in place across the school, ensuring that staff and students receive different levels of filtered internet access in line with user requirements.
- All users have unique usernames and passwords to access the school network which ensures that they receive the appropriate level of filtering. Class log-ins, dependent on age, may also be used.
- Any changes to filtering levels are documented on the IT Helpdesk and include the reason for the requested change, the date and name of staff member concerned.

In addition to the above, the following safeguards are also in place

- Anti-virus and anti-spyware software is used on all network and stand-alone PCs of laptops and is updated on a regular basis.
- A firewall ensures that information about students cannot be accessed by unauthorised users.
- Encryption codes on wireless systems prevent hacking.
- The CEOP Report Abuse link is available on the school VLE to allow students or staff to report online safeguarding issues.

Staff

- Expectations for staff online conduct is addressed in the Acceptable Use Policy for School based employees and Email Etiquette document.
- Staff are required to preview any websites before use, including those which are recommended to students and parents for homework support.

The Prevent Duty (Protecting Young People from Radicalisation)

The school takes seriously its responsibility to prevent students from being drawn into extremist activities in all contexts.

All students are entitled to protection against all messages of violent extremism using any means or medium to express views that:

- encourage, justify or glorify political, religious, sexist or racist violence
- subscribe to rigid and narrow ideologies that are intolerant of diversity, leaving those who hold them vulnerable to future radicalization
- foster hatred which might lead to inter-community violence in the UK
- seek to provoke others to terrorist acts
- encourage other serious criminal activity or seek to provoke others to serious criminal acts

The school aims to build awareness of extremism and to enable our students to challenge extremist views. We do not stop the debating of controversial issues, but instead provide a safe space in which students and staff can raise these issues, understand the associated risks and develop the knowledge, skills and understanding to be able to respond to extremism.

Staff Training:

- The School's Designated Safeguarding lead will undertake Prevent awareness training and will able to provide advice and support to other members of staff on protecting children from the risk of radicalisation.
- All teachers should complete the online general awareness training module on the Channel programme which includes how to identify factors that can make people vulnerable to radicalisation, and case studies illustrating the types of intervention that may be appropriate, in addition to Channel.

Any member of the school community who has concerns that extremist or radical activity could be affecting anyone in the school is encouraged to contact the School's Designated Safeguarding lead (Mr R. King) immediately.

Use of School and Personal ICT Equipment

School ICT Equipment

- A log of all ICT equipment issued to staff, including serial numbers, is maintained by the Network Manager.
- Personal or sensitive data is not stored on school devices (e.g. laptops, ipads, PC or USB Memory Sticks) unless encryption software is in place. This is true also of any photographs or videos of students, such as class photos or assembly evidence. All such material should be stored either on the school network or on an encrypted device.
- Time locking screensavers are in place on all devices in school to prevent unauthorised access, particularly on devices which store personal or sensitive data. Personal ICT equipment, such as laptops or memory sticks, must not be connected to the school network without explicit consent from the Network Manager or ICT Co-ordinator and a thorough virus check. Staff and student personal equipment (laptops, tablets, phones etc.) will not be allowed onto the schools network if they pose a threat to the security of the network. Equipment that is already connected to the school network and has become a threat will also be removed.

The use of mobile phones/devices, memory sticks and photography in school is detailed in the Acceptable Use Policy.

Parent/ Involvement

As part of the school's commitment to developing e-safety awareness amongst students and staff, every effort is made to engage parents in the process.

- All students and their parents will receive a copy of the Acceptable Use Policy? on entry to the school. Students and their parents are asked to read and sign acceptance of the rules, a copy of which is stored in school.
- All staff and students have to agree to the Acceptable Use Rules whenever they logon to the school network.

On request, the school will provide parents without internet access the means to research online materials and resources.