E-Safety Policy

Love, Learn and Shine Together with Jesus

Written: February 2020

Date of Review: February 2024

Leader: Mr Garcia

St Matthew's E-Safety Policy

1. Introduction and Overview

The purpose of this policy is to:

- Outline the guiding principles for all members of the school community regarding the use of ICT.
- Safeguard and protect the students and staff and help them to work safely and responsibly with the internet and other communication technologies.
- Set clear expectations of behaviour relating to responsible use of the internet and technology for educational, personal or recreational use.
- Establish clear reporting mechanisms to deal with online abuse such as bullying that are cross referenced with other school policies.
- Ensure that all members of the school community know that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

Scope of the policy
This policy applies to all members of school community - staff, students, volunteers, parents and carers, visitors, community users - who have access to and are users of school's ICT systems.

Communication of the policy
The policy will be communicated to the school community in the following ways:

- Displayed on the school website, and available in the staffroom and classrooms.
- Included as part of the induction pack for new staff.
- Acceptable use agreements discussed with and signed by students at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school.
- Acceptable use agreements to be held in student and personnel files.

Responding to concerns

- The school will take all reasonable precautions to ensure internet safety. However, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of internet access.
- Staff and students are informed of the possible sanctions related to misuse of technology and these are outlined in the Positive Behaviour and Relationship Policy.
- Our Safeguarding team is the first point of contact for any concerns. Any concerns about staff misuse will be referred to the Headteacher.

- Concerns that relate to online bullying will be dealt with in line with our Anti-Bullying Policy. Concerns related to child protection are dealt with in line with the school child protection procedure.

Review and Monitoring
Internet safety is integral to other school policies including the Computing Policy, Child Protection Policy, Anti-Bullying Policy and Behaviour Policy.

The school's Senior Management is responsible for writing, reviewing and updating the policy. The policy will be reviewed annually or more frequently in response to changing technology and internet safety issues in the school.

This policy has been developed in consultation with the school's IT Coordinator Pastoral Care Manager and approved by the Senior Leadership Team and Board of Governors. Staff will be informed of any updates or amendments to it.

2. Education and Curriculum

Student Internet Safety curriculum

The school has a clear, progressive internet safety education programme primarily as part of the Computing / PSHE curriculum but referenced in all areas of school life. In EYFS and KS1 we use a DigiDog soft toy character in each class to teach the children online safety. Each week throughout the term DigiDog is allowed to visit a child's home. The activities, conversations and feedback that arise from this keeps the important online safety messages ever present throughout the school year. We run an e-Cadet Program where peer to peer teaching around e-safety takes place. We do a whole school celebration for Internet Safety Day each year and provide a variety of enrichment activities covering a range of skills and behaviours appropriate to students' ages and experience, including:

- Digital literacy.
- Acceptable online behaviour.
- Understanding of online risks.
- Privacy and security.
- Reporting concerns.

The school will:

- Plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Remind students about their responsibilities using the Acceptable Use Policy signed by every student.
- Ensure that staff model safe and responsible behaviour in their own use of technology during lessons.

- Ensure that staff and students understand issues around plagiarism and copyright/intellectual property rights, and understand how to critically assess the validity of the websites they use.

Staff and governor training

The school will ensure that:

- Staff understand the requirements of the Data Protection Act in terms of sending and receiving sensitive personal information.
- Regular training is available to staff on internet safety issues and the school's internet safety education programme.
- Information and guidance on the Safeguarding policy and the school's Acceptable Use Policy is provided to all new staff and governors.

Parent engagement

The school recognises the important role parents and carers have in ensuring children and young people are safe, responsible and can flourish online. To support parents to understand online risks and the work of the school in this area we will provide:

- Acceptable Use Agreements to all new parents.
- Regular, up to date information in newsletters and on the website and social media, particularly in response to emerging trends.
- Face to face sessions in school.
- Opportunities to share in their children's internet safety learning (e.g. assemblies, performances).
- Support and advice on online safety for their children outside of school.
- Signposting to further resources and websites.

3. Conduct and Incident management

Conduct

All users are responsible for using the school ICT systems in line with the Acceptable Use Policy they have signed. They should understand the consequences of misuse or access to inappropriate materials.

All members of the school community should know that this policy also covers their online activity outside of school if it relates to their membership of the school.

Parents and carers will be asked to give consent for their children to use the internet and other technologies in school, by signing an Acceptable Use Agreement. They will also be given clear information about the sanctions that might result from misuse.

Incident Management

All members of the school community understand they have a responsibility to report issues and are confident that anything raised will be handled quickly and sensitively, in line with the school's Misuse Plan. The school actively seeks advice and support from external agencies in handling internet safety issues. Parents and carers will be informed of any internet safety incidents relating to their own children.

4. Managing the ICT infrastructure

The school is responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that related policies and procedures are implemented. It will also ensure that the relevant people will be effective in carrying out their internet safety responsibilities with regards to the ICT infrastructure.

- The technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of the school's technical systems.
- All users will have clearly defined access rights to the technical systems and school owned devices.
- All staff have individual logins and passwords.
- Where appropriate all pupils have individual logins and passwords for various learning platforms.
- The administrator passwords for the school ICT system, used by the Network Manager is also available to the Headteacher and kept in a secure place.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The school allows different filtering levels for different groups of users – staff / students.
- The school can monitor and record the activity of users on the school technical systems and users are made aware of this.
- There is a reporting system in place for users to report any technical incident or security breach.
- Security measures are in place protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Social Media

St Matthew's has a Staff Social Media Policy and a Pupils/Parents/Visitors Social Media Policy that covers the management of school accounts and set out guidelines for personal use of social media.

5. Data

The school has a Data Protection and Handling Policy that is regularly reviewed and updated. This includes information on the transfer of sensitive data; the responsibilities of the Senior Information Risk Officer; and the storage and access of data.

6. Equipment and Digital Content

Personal mobile phones and mobile devices – please see school Mobile Phone Policy.

Digital images and video

All schools need and welcome positive publicity. Photographs of pupils can add colour, life and interest to articles promoting school initiatives and activities. Making use of photographs in school publicity materials can increase pupil motivation and staff morale. Parents and carers, members of the Governing Body and the local community can identify and celebrate the work and achievements of the school. A photographic record of school events can also be a useful historical record of the school's work over a long period of time. However, photographs need to be taken and used in a responsible way.

We will seek permission from parents and carers for the use of digital photographs or video involving their child in accordance with our Safe Use of Children's Photographs Policy Agreement when their child joins the school.

Students are taught to think carefully about placing any personal photos on social media sites. The importance of privacy settings as a tool to safeguard their personal information is included in internet safety education. They are also taught that they should not post images or videos of others without their permission.

Students understand the risks associated with sharing images that reveal the identity of others and their location, such as house number, street name or school.