Section 3.6 **St Saviour's & St Olave's Online Safety Policy**

Mission statement

St Saviour's & St Olave's school is a church school and the Governing Body seeks to ensure that the Christian ethos permeates the whole life of the school. This policy is designed to ensure that all those within the school community are protected from the possible risks of working online. An integral part of this is ensuring that all members of our community are well informed and receive suitable education on adhering to and working within safe and responsible guidelines. The effective application of this policy relies on the commitment of every individual working together.

Introduction

This policy applies to all members of the school community (including staff, students, volunteers, governors, parents/carers and visitors) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

It is expected that all members of the school community will be responsible users of digital technology, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. The school has clear guidelines on the appropriate use of computer equipment and online activities. This is set out in the schools' acceptable use policy and is signed by staff, students and parents annually. Any incidents or concerns should be reported to the online safety coordinator or the Head teacher.

Roles and Responsibilities

The roles of individuals in dealing with online safety issues are in line with those outlined in the school safeguarding policy. Overall responsibility in decision making and dealing with incidents falls with the Head teacher and the Governors. However, everyone within the school community has a role in ensuring that computer equipment and the online domain is used in a responsible manner and its users are safe. The roles of groups and individuals are explained in more detail in the process manual that helps to implement elements in this policy.

Policy Statements

Education – students

Students need to be taught to take a responsible approach to using any digital device and the education of students in this areas is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be reflected in all areas of the curriculum and staff should reinforce messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- Planned online safety units should be provided as part of Computing / PHSE and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for a Student Acceptable Use Policy and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.

- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can make a request to the online safety coordinator for consideration to temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers

Some parents and carers may only have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children’s online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website
- Parents / Carers sessions
- High profile events or campaigns e.g. Safer Internet Day
- Reference to the relevant web sites and publications

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policy.
- The Online safety Coordinator (or other nominated person) will receive regular updates through attendance at external training and by reviewing guidance documents released by relevant organisations.
- This Online safety policy and its updates will be presented to and discussed by staff.

Training – Governors

The school Governors will monitor the programme of online safety training and attend sessions where appropriate.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure and IT network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- School 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 school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password
- The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Head teacher or other nominated senior leader and kept in a secure place.

- Technical staff are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users.

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. Any member of staff bringing in and using such devices must follow the same guidelines as those given for using any item of computer equipment in school. Please note the current school policy states that students in years 7-11 are not allowed to bring their own devices into school.

Use of digital and video images

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites. Students should be made aware that the sharing of images without the permission of those in the photograph is not permitted.

Written permission from parents or carers is obtained when students join the school which gives permission for photographs of students to be published on the school website. Individuals are never identified by name in published photographs.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Full details of this can be found in the schools' data protection policy

Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carers must be professional in tone and content. This contact should only be done using staff school email accounts.
- Students will be provided withindividual school email addresses for educational use. This is the only email account that students should use when contacting staff about their work. Any emails sent to staff from students' personal email accounts should not be responded.
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

We have a duty of care to provide a safe learning environment for students and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully or discriminate on the grounds of sex, race, disability, religion or belief, sexual orientation, gender reassignment, pregnancy or maternity or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk
- No reference should be made in social media to students, parents/carers or school staff

- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Updated June 2019