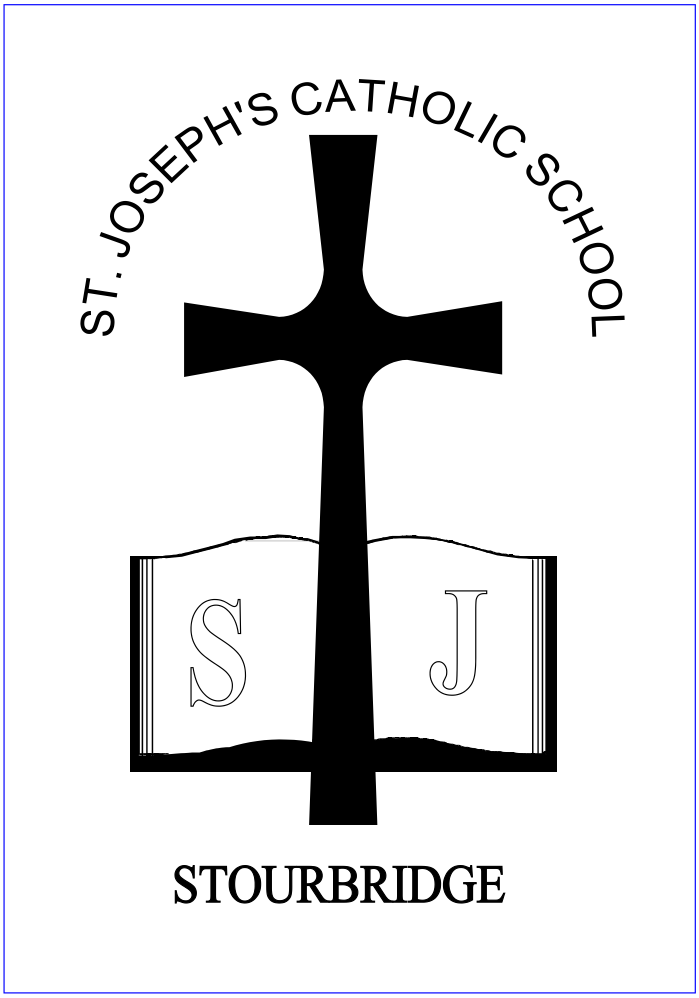


Online Safety Policy

July 2018

School Mission Statement

In following the Gospel values of Jesus, we are called to love, to learn and to respect one another.

Education – students / pupils

There is a planned and progressive Online safety. Learning opportunities are embedded into the curriculum throughout the school and are taught in all year groups. All staff have a responsibility to promote good Online/E-safety practices.
Online safety/E-Safety education is provided in the following ways:

- A planned Online safety/E-Safety/E-literacy programme is provided as part of Computing / PHSE and is regularly revisited – this includes the use of ICT and new technologies in and outside the school
- Key Online safety/E-Safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy and plausibility of information
- Pupils are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside the school
- Pupils are aware that their network activity is monitored and where pupils are allowed to freely search the internet their internet activity is being scrutinised
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet are posted in all rooms
- Pupils are taught the importance of information security and the need to keep information such as their password safe and secure
- Staff act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

The school provides information and awareness to parents and carers through newsletters and the school website.

Education - Extended Schools/Wider Community

The school offers family learning courses in ICT, computing, digital literacy and Online safety/E-Safety so that parents/carers and children can together gain a better understanding of these issues. Messages to the public around Online safety/E- Safety are targeted towards grandparents and other relatives as well as parents/carers.
Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training – Staff

All staff receive regular Online safety/E-Safety training and understand their responsibilities, as outlined in this policy. Training is offered as follows:

- A planned programme of formal Online safety/E-Safety training is made available to staff. An audit of the Online safety/ E-Safety training needs of all staff is carried out regularly.
- All new staff receive Online safety/E-Safety training as part of their induction programme, ensuring that they fully understand the school Online safety/E-Safety Policy and Acceptable Use Agreements
- The Principal receives regular updates through attendance at DGfL / LA training sessions and by reviewing guidance documents released by DfE / DGfL / LA.
- This Online safety/E-Safety policy and its updates are presented to and discussed by staff in INSET days

All staff are familiar with the school/academy policy including:

- Safe use of e-mail
- Safe use of the internet including use of internet-based communication services, such as instant messaging and social network or any other school/academy approved system
- Safe use of the school network, including the wireless network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- Publication of pupil information/photographs/videos/posts/blogs/calendars and information available on the school/academy website
- Capturing and storing photographs/videos/audio files on personal and school/academy owned devices
- Cyberbullying procedures
- Their role in providing Online safety/E-Safety education for pupils
- The need to keep personal information secure

All staff are reminded / updated about Online/E-Safety matters at least once a year.

Training – Governors/Directors

Mrs Price, Academy Committee Link Representative, takes part in Online safety / E-Safety training / awareness sessions.

.

This is offered by:

- Attendance at training provided by the Local Authority / National Governors Association / DGfL/ LSGB or other relevant organisation
- Participation in school/academy training / information sessions for staff or parents
- Invitation to attend lessons, assemblies and focus days

Technical – infrastructure / equipment, filtering and monitoring

The managed service provider is responsible for ensuring that the school/academy 'managed' infrastructure / network is as safe and secure as is reasonably possible. The school/academy is responsible for ensuring that policies and procedures approved within this document are implemented.

Filtering

DGfL filtering is provided by Smoothwall. The IWF (Internet Watch Foundation) list and the "police assessed list of unlawful terrorist content, produced on behalf of the Home Office", is integrated into the Smoothwall database.

Web filtering policies are applied based on:

"who" (user or user group from a directory),

“what” (type of content),
“where” (client address – either host, subnet or range),
“when” (time period) in a filtering policy table that is processed from top-down

Monitoring
DGfL’s monitoring solution is provided by e-Safe. e-Safe’s detection technology monitors imagery, words and contextual phrases, during online and offline activity, to identify behaviour which may represent a safeguarding risk or breach of acceptable use policies.

School ICT systems will be managed in ways that ensure that the school/academy meets the Online/E-Safety technical requirements outlined in the Acceptable Use Agreement Policy.

- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted to authorised users

All users will have clearly defined access rights to school/academy ICT systems

- All users will be provided with a username and password
- Users will be made responsible for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The school maintains and supports the managed filtering service provided by DGfL.
- The school manages and updates filtering issues through the RM Service desk
- Requests from staff for sites to be removed from the filtered list will be considered by the Mrs McCole. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by SLT.
- An appropriate system is in place for users to report any actual / potential Online safety/E-Safety incident to the relevant person
- The managed service provider ensures that appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school
- An agreed procedure is in place for the provision of temporary access to “guests” (e.g. trainee teachers, visitors) onto the school
- An agreed procedure is in place regarding the extent of personal use that users (staff) and their family members are allowed on school owned laptops and other portable devices that may be used out of the school
- An agreed procedure is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school/academy workstations / portable devices
- 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 site unless safely encrypted or otherwise secured
- The school has responsibility for ensuring files and applications accessed via CC4 Anywhere or a similar application, comply with information and data security practices

Curriculum

Online/E-Safety is a focus in all areas of the curriculum. The Computing Curriculum specifically identifies 'Digital Literacy' as a focus. Digital Literacy is taught. Staff will re-enforce Online safety/E-Safety messages in the use of ICT across the curriculum and during Computing lessons.

- In lessons, where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and there are processes in place for dealing with any unsuitable material that is found in internet searches
- Where students / pupils are allowed to freely search the internet, e.g. using search engines, staff should monitor the content of the websites the young people visit
- The school provides opportunities within a range of curriculum areas to teach about Online/E-Safety
- The school teaches 'Digital Literacy' as part of the Computing programme of study
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- Students / pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Pupils are aware of the impact of Cyberbullying, Sexting and Sextortion, Revenge Porn and Radicalization and know how to seek help if they are affected by any form of online bullying or exploitation. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button

Use of digital and video images

When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, and follow school/academy policies concerning the storing, sharing, distribution and publication of those images. Those images are only taken on school equipment, the personal equipment of staff are not used for such purposes
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However, with the express permission of the Principal, images can be taken provided they are transferred immediately and solely to the school's/academy's network and deleted from the pupil's device.
- Care is taken when capturing digital / video images, ensuring students / pupils are appropriately dressed and that they are not participating in activities that might bring the individuals or the school into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and comply with good practice guidance on the use of such images
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers is obtained before photographs of pupils are published on the school website
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school

events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.

Data Protection (General Data Protection Regulations)

The school has a Data Protection Policy that meets statutory guidance.

Personal data is recorded, processed, transferred and made available according to the General Data Protection Regulations (GDPR) which states that personal data must be:

- Fair and transparent (privacy notice)
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

A breach of GDPR may result in the school / company being fined up to 4% of its annual turnover or 20,000,000 euros.

Staff ensure that they:

- Take care at all times, to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Access personal data on secure password protected computers and other devices, at the school and home, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected *(many memory sticks / cards and other mobile devices cannot be password protected.)*
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school/academy policy once it has been transferred or its use is complete.

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. Staff and pupils should therefore use only the school email service to communicate with others when in the school or on school systems e.g. by remote access from home- *(If staff use none standard or personal email accounts these are not secure and cannot always be monitored)*
- Users need to be aware that email communications may be monitored

- Users must immediately report, to Mrs McCole– in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and pupils or parents / carers (email, chat, school VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications
- Pupils are provided with individual school email addresses for educational use from Year 3. Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the school website, on public facing calendars and only official email addresses should be used to identify members of staff
- Mobile phones may be brought into the school by pupils but are left in the school office
- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances should a member of staff contact a pupil or parent/ carer using their personal device about issues concerning school unless authorised to do so by the school
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Users bringing personal devices into the school must ensure there is no inappropriate or illegal content on the device

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. The school has a policy that sets out clear guidance for staff to manage risk and behaviour online. 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
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, 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.

Unsuitable / inappropriate activities

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the GDPR Regulations 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000. The school will take all reasonable precautions to ensure Online safety/E-Safety is a key focus.
However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.

Staff and pupils are given information about infringements in use and possible sanctions.

Sanctions available include:

- Interview / counselling by Principal or Vice Principal
- Informing parents or carers
- Removal of Internet or computer access for a period, (which could ultimately prevent access to files held on the system, including examination coursework).
- Referral to LA MASH
- School policies include infringements relating to online activities (Behaviour policy, Anti-bullying policy, Child Protection policy)

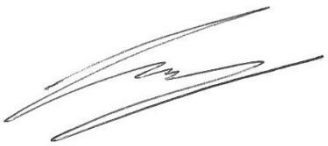
Our E-Safety Coordinator, Mrs McCole, acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Principal (Mr Carry).

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school, LSCB child protection procedures.

There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

Date: July 2018

Date for review: July 2019

Signed (Principal): 

Signed (Chair of the Academy Committee):