St. Julian's School Online Safety Policy

Contents

Introduction

This school Online Safety Policy is intended to consider all current and relevant issues, in a whole school context, linking with other relevant policies, such as the Safeguarding & Child Protection Policy, Behaviour Policy, Mobile Phone Policy and the Anti-Bullying policy.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. St. Julian's School, through this Online Safety Policy, ensures that we meet our statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. The policy will also form part of the school's protection from legal challenge, relating to the use of digital technologies.

Due to the ever changing nature of digital technologies, this policy will be reviewed annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Board of Governors on:	*June 14th 2022*
The responsibility for the implementation of this Online Safety policy ilies with:	*Director of Technology and the SJS Safeguarding Team*
Monitoring will take place at regular intervals:	*Once a year*
The Board of Governors will receive a verbal report from the Safeguarding Governor on the implementation of the Online Safety Policy (which will include anonymous details of online safety incidents) at regular intervals:	*Once a term*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*june 14th 2023*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys / questionnaires of
    - students
    - parents / guardians
    - staff

Scope of the Policy

This policy applies to all members of the St. Julian's School community (including staff, students, volunteers, parents / guardians, visitors, community users) who have access to and are users of the school's Information and Communication (ICT) systems, both in and out of the school.

The school will deal with such incidents within this policy and associated child protection, behaviour and anti-bullying policies and will, where known, inform parents / guardians of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. The Safeguarding Governor will meet as necessary with the Director of Technology and the Director of Student Support to be informed of any serious online incidents that affect child safety. The Governor will include online safety updates, as part of the scheduled termly Board updates on child safeguarding.

Head of School / Senior Leaders:

- The Whole School Leadership Team (WLT) has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Head of School and (at least) another member of the Whole School Leadership Team (WLT) should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, or students.
- The Head of School is responsible for ensuring that the Technology Director and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. The Head of School will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support those colleagues who take on important monitoring roles.
- The Whole School Leadership Team will receive regular monitoring reports from the Director of Technology.

Safeguarding Team:

- Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
    - sharing of personal data
    - access to illegal / inappropriate materials
    - inappropriate on-line contact with adults / strangers

    - potential or actual incidents of grooming
    - cyber-bullying
- has a consulting role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident relating to safeguarding taking place
- provides safeguarding training and advice for staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- keeps relevant stakeholders informed

Technology Director / Head of IT Services:

The Technology Director and Head of IT Services are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that the filtering policy is applied and updated on a regular basis and shared with the Whole School Leadership Team.
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network and school platforms can be monitored in order that any misuse / attempted misuse can be reported to the WLT; Safeguarding Team

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current St. Julian's Online Safety Policy and practises
- they have read, understood and signed the Staff Acceptable Use Policy Agreement (AUP)
- all digital communications with students / parents / guardians should be on a professional level and only carried out using official school systems

- online safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the Online Safety Policy and Acceptable Use Policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices

Students / Pupils:

- are responsible for using the St. Julian's digital technology systems in accordance with the relevant Student Acceptable Use Agreement
- have a good understanding of academic honesty, research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *school's* Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / guardians

Parents / guardians play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, workshops, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and guardians will be encouraged to support the School in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the parent portal
- their children's personal devices in the school (where/when permitted)

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety 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 a focus in all areas of the curriculum and staff should reinforce online safety 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:

- A planned online safety curriculum should be provided as part of Computing / H&C / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / 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 supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students should be helped to understand the need for the student Acceptable Use Agreement 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 request that the Technical Staff (or other relevant designated person) can 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 / guardians

Many parents and guardians have only 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 on-line 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 guardians through:

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents workshops
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-guardians *https://www.seguranet.pt/pt/pais*

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 Agreements.
- It is expected that some staff will identify online safety as a training need

within the professional learning and growth cycle..

- The Safeguarding Team will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Safeguarding Team will provide advice / guidance / training to individuals as required.

Training – Governors / Directors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training by external providers.
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- 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 where possible
- All users will have clearly defined access rights to school technical systems and devices.
- All staff users will be provided with a username and secure password by the IT team *who* will keep an up to date record of users and their usernames. Staff will be required to change their password at least once a year..

- All students (at Year 4/3º ano and above) will be provided with a username and secure password by the IT team *who* will keep an up to date record of users and their usernames. They are responsible for the security of their username and password and will be required *to* change their password once every year. All KS3 students are also required to change their iPad passcode at least once a year.
- Students up to year 4/3º ano will be provided with a username and secure password by the IT team *who* will keep an up to date record of users and their usernames. These passwords will be changed once a year by the IT support team and students will be informed of their new password.
- The administrator passwords for the school ICT system, used by the Head of IT Services must also be available to the Head of School
- The Head of IT Services is 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. Illegal content (child sexual abuse images) is filtered by our Cisco Umbrella service. Content lists are regularly updated and internet use is logged and monitored on request by WLT / Governors. There is a clear process in place to deal with requests for filtering changes
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Users can report any actual / potential technical incident / security breach to the relevant person via IT Support request (email).
- Appropriate security measures are in place to 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.
- An isolated network is in place to provide temporary access to guests onto the school systems via IT Support request.
- Agreed policies are in place (Acceptable Use Policies) regarding the extent of personal use that users (staff / students / community users) and their family members are allowed on school devices that may be used out of school.
- Removable storage media (eg memory sticks / CDs / DVDs) should not be used by users on school devices.

Mobile Technologies (including BYOD)

Mobile technology devices may be school provided by the school or personally owned and might include: smartphone, tablet, laptop, smartwatch or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile / personal devices in a school context is educational. The Mobile Phone Policy should be understood alongside the other relevant school policies including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education programme.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / guardians and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- 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.
- Written permission from parents or guardians will be obtained before photographs of students are published on the school website / social media / local press. The list of these students is contained in the school's

MIS.

- In accordance with standard practice under the GDPR, parents / guardians are welcome to take videos and digital images of their children at school events for their own personal use (as such use not covered by the GDPR). 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 / guardians comment on any activities involving other students in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school procedures concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, newsletters or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website, newsletters, social media etc. particularly in association with photographs.
- Student's work can only be published with the permission of the student and parents or guardians.

Data Protection

Personal data will be recorded, processed, transferred and made available according to GDPR Standards, the school's Data Protection Policy and local Portuguese data privacy law 58/2019 which states that personal data must be:

- Fairly and lawfully processed
- 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.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The use of communication devices within school should be considered in relation to the Mobile Devices Policy

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

- The official St. Julian's School email service may be regarded as safe and secure. Staff and students should use only the school email service to communicate with others for educational purposes
- Users must immediately report, to the Head of School, 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. If the Head of School is the offender, the Chair of the Board should be notified.
- Any digital communication between staff and students or parents / guardians (email, social media, Google Chat, Google Classroom etc) must be professional in tone and content. Personal messaging (email, text or social media) must not be used for these communications.
- 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

The School has a duty of care to provide a safe learning environment for students and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. 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:

- Ensuring that personal information is not published
- Training is provided including: 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

School staff should ensure that:

- No reference should be made in personal social media to students, parents / guardians 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
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- A process for approval by WLT
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to proactively monitor the Internet for public postings about the school

- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by the Communications Team and Technology Director to ensure compliance with the school policies.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and are obviously banned from school and all other technical systems. Other activities e.g. cyber-bullying are banned and could lead to criminal prosecution. 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.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities. Any incidents involving safeguarding or child protection issues should be dealt with in line with the Safeguarding & Child Protection Policy

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, this must be reported to the safeguarding team via the safeguarding concerns procedure.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, 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.

In the event of suspicion, steps outlined in the school's Behaviour Policy will be implemented and in addition the following procedure will be carried out.

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- If content being reviewed includes images of Child abuse then the monitoring should be halted, and referred to the Police immediately. For other instances, the Head of School should be consulted to determine if a report to the police should be made. These would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - Racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- In these situations, isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with in conjunction with the school's Behaviour Policy.

Appendix

Additional documentation:

Student Acceptable Use Agreement (Older students)

Student Acceptable Use Agreement (Foundation and KS1)

Staff Acceptable Use Agreement

iPad Agreement

Mobile Phone Policy

Behaviour Policy

Safeguarding & child protection policy

Data Protection Policy

Review Date	Amendment	Approved by
June 14, 2022	**New policy**	**BOG**