St. Joseph's Catholic College

Online Safety Policy 2020

Monitoring

By	Review period	Method
Governing Body	Annual	Meeting

Ownership: Assistant Principal responsible for Pastoral and Network Manager

Revision History

Review	Changes	Next review date
February 2020	Update terminology and refereneces	February 2021

Ownership: eSafety Co-Ordinator
E-Safety Group

Role	Name
E-Safety Co-ordinator	Adrian Stoten
E-Safety Link Governor	Elizabeth Barrett
Network Manager	Alexander Cann

Scope of the Policy
The College's responsibilities around online safety are highlighted in the recent DfE advice:

Keeping Children Safe in Education (Sept 2019) states:
"Governing bodies and proprietors should ensure that children are taught about safeguarding, including online safety."

More detailed advice on the delivery of online safety has been published in "Teaching Online Safety in Schools." (non-statutory guidance June 2019)

This policy applies to all members of the College's community (staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of the College's digital technology systems, both in and out of the College.

The Education and Inspections Act 2006 empowers the Principal to regulate the behaviour of students when they are off the College's site and empowers members of staff to impose disciplinary penalties for in appropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy(as outlined in KCSIE 2019), which may take place outside of the College, but is linked to membership of the College. The 2011 Education Act increased these powers with regard to the search for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The College 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 the College. The College will also deal with incidents that fall under the Prevent Duty remit, as outlined in Channel Guidance (December 2019).

Roles and Responsibilities

1. **Governors** are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. The governing body will receive regular information about online safety incidents and monitoring reports. This will be included in the regular student report. The Designated Governor for Safeguarding will monitor online safety through:
    a. Regular meetings with the Online Safety Co-ordinator
    b. Regular monitoring of online safety incident logs
    c. Regular monitoring of filtering logs

2. **The Principal** has a duty of care for ensuring the safety (including online safety) of members of the College's community, through day-to-day

responsibility for online safety will be delegated to the Online Safety Co-ordinator.

3. **The Principal and the Designated Senior Manager for Allegations** should be aware of procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see Safeguarding Policy).

4. **The Principal and the Designated Safeguarding Lead** are responsible for ensuring that the Online Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues as relevant.

5. **The Principal and Designated Safeguarding Lead** will ensure that there is a system in place to allow for the monitoring and support of those in the College who carry out the internal online safety role, in order to provide a safety-net and also support colleagues who have important monitoring roles.

6. **The Onlline Safety Co-ordinator** will
    a. Lead the Online Safety Board
    b. Take day-to-day responsibility for online safety issues and have a leading role in establishing and reviewing College online safety documents and procedures.
    c. Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
    d. Provides training and advice for staff.
    e. Liaises with LA.
    f. Liaises with the College's technical staff.
    g. Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments. This log is kept in the Pastoral area.
    h. Meets with the Safeguarding Governor at Safeguarding Alignment Meetings to discuss current issues, review incident logs and filtering logs.
    i. Attends relevant Governor meetings.
    j. Reports regularly to the Senior Leadership Team.

7. **The Network Manager / Technical staff** are responsible for ensuring:
    a. That the College's technical infrastructure is secure and is not open to misuse or malicious attack.
    b. That the College meets required online safety technical requirements and any other guidance that may apply.
    c. That users may only access the networks and devices through a properly enforced password protection policy in which passwords are regularly changed.
    d. The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
    e. That the use of the network/internet/VLE/remote access/email is regularly monitored in order that any misuse or attempted misuse can be reported to the Principal/Designated Senior Manager for

Allegations/Online Safety Co-ordinator for investigation/action/sanction.

f. That monitoring software/systems are implemented and updated as agreed in the College's Information Security and IT Acceptable Usage Policies.

8. **Teaching and Support Staff** are responsible for ensuring that:
    a. They have an up-to-date awareness of online safety matters and of the current College e-safety policy and practices.
    b. They have read, understood and signed the Staff Acceptable Use Policy.
    c. They report any suspected misuse or problem to the Principal/Online Safety Co-ordinator for investigation/action/sanction.
    d. All digital communications with students/parents/carers should be on a professional level and only be carried out using official College systems.
    e. E-safety issues are embedded in all aspects of the curriculum and other activities.
    f. Students understand and follow the e-safety and acceptable use policies.
    g. Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
    h. They monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other College activities and implement current policies with regard to these devices.
    i. In lessons where Internet use is pre-planned, 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.

9. **Designated Safeguarding Lead and Deputies** should be trained in online safety issues and be aware of potential for serious child protection/safeguarding issues to arise from:
    a. Sharing of personal data
    b. Access to illegal/inappropriate materials
    c. Inappropriate on-line contact with adults/strangers
    d. Potential or actual incidents of grooming
    e. Cyber-bullying

10. **OnlineSafety Group** provides a consultative group that has wide representation from the College community with responsibility for issues regarding e-safety and monitoring the online safety policy, including the impact of initiatives. Members of this group are part of the Safeguarding Team. This group is responsible for reporting to Governors. This group will assist the Online Safety Co-ordinator with:
    a. the production, review and monitoring of the College's online safety policy
    b. the production, review and monitoring of the College's filtering policy and requests for filtering changes
    c. mapping and reviewing online safety curricular provision

d. monitoring network/internet/incident logs
e. consulting stakeholders about online safety provision
f. monitoring improvement actions identified through use of the 360 degree safe self review tool.

11. **Students** are responsible for using the College's digital technology systems in accordance with the Acceptable Use Policy. They:
    a. Should have good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
    b. Need to understand the importance of reporting abuse, misuse or access to in appropriate materials and know how to do so.
    c. Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand the policies on taking/use of images and on cyber-bullying.
    d. Should understand the importance of adopting good online safety practice when using digital technologies out of College and realise that the College's Online Safety Policy covers their actions out of College, if related to membership of the College.

12. **Parents/Carers** play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The College will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about online safety campaigns. Parents/carers will be encouraged to support the College in promoting good online safety practice and to follow guidelines on appropriate use of:
    a. Digital and video images taken at College events.
    b. Access to parents' sections of the website/VLE and online student records.
    c. Their children's personal devices in the College.

13. **Community Users** who access the College's systems/website as part of the wider College will be expected to sign a Community User AUA before being provided with access to College systems.

Policy Statements

Education – Students

Online safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum, helping students to recognise and avoid e-safety risks and build their resilience. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities. This will be provided in the following ways:

- A planned online safety curriculum as part of Computing/PSHE/other lessons 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 online 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 the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside of the College.
- In lessons where internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of websites visited.
- It is accepted that occasionally, for good educational reasons, students may need to research topics that would normally result in internet searches being blocked (e.g. drugs, racism, discrimination). In such circumstances, staff may request that IT technicians can temporarily remove those sites from filtered lists for the period of study. Any request to do so should be auditable with clear reasons for the need.

Misuse of the ICT systems are dealt with within the College's behaviour policy. Where suitable sanctions for misuse are defined.

Education – Parents/Carers
Many parents/carers may have only a limited understanding of online safety risks, yet play an essential role in the monitoring and regulation of their children's on-line behaviours. The College will, therefore, seek to provide information and awareness to parents/carers through letters, newsletters, website, VLE, parents' evenings, reference to websites and publications.

Education – The Wider Community
The College will provide opportunities for members of the local community to gain from the College's online safety knowledge and experience. This may be offered through the following:
- Providing online safety information for the wider community.
- Supporting community groups (e.g. partner primaries) to enhance their online safety provision.

Education and Training – Staff/Volunteers
It is essential that all staff receive online safety training and understand their responsibilities. Training will be offered as follows:
- A planned programme of formal online safety training that 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 College's Online Safety Policy and Acceptable Use Agreement.

- The Online Safety Co-ordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- Online safety policies and updates will be presented to and discussed by staff in staff meetings and Inset days.
- The Online Safety Co-ordinator will provide advice/guidance/training to individuals as required.

Training – Governors
Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any subcommittee involved in technology/e-safety/health and safety/child protection. This may be provided through LA or National Governors Association, or through participation in College training for staff or parents.

Technical – infrastructure/equipment filtering and monitoring
The IT Support Team will be responsible for ensuring that the College's 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 e-safety.

- There will be regular reviews and audits of the safety and security of College technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to the College's technical systems and devices.
- All users will be provided with a username and secure password by the Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every three months.
- The "master / administrator" passwords for the College's ICT system, used by the Network Manager must also be available to the Director of Finance and kept in a secure place.
- The Network Manager 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 the filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. All requests for filtering changes must be logged on the IT helpdesk and approved by SLT.
- The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / students, etc.)

- The College's technical staff regularly monitor and record the activity of users on the College's technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the IT Support Team. This system is known as Securus.
- 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 College systems and data. These are tested regularly. The College infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the College systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / community users) and their family members are allowed on College devices that may be used out of College. This is defined in the IT Acceptable Use Policy.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on College devices. This is defined in the Information Security Policy.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on College devices. Personal data cannot be sent over the internet or taken off the College site unless safely encrypted or otherwise secured. This is also defined in the Information Security Policy.
- An agreed procedure is in place for defining filtering protocols for academic access. Requests must be made by a member of staff to the IT Support Team. Any concerns are then reported to the Team's line managers, who will then refer to the academic section of the Senior Leadership Team.

Bring Your Own Device

- The College has a set of clear expectations and responsibilities for all users, as outlined in the staff Code of Conduct and the Behaviour Policies.
- The College adheres to the Data Protection Act principles.
- All users are provided with and accept the Acceptable Use Agreement.
- All network systems are secure and access for users is differentiated.
- Where possible these devices will be covered by the College's normal filtering systems, while being used on the premises.
- All users will use their username and password and keep this safe.
- Training relating to BYOD and Data Protection is undertaken for all staff.
- Students receive training and guidance on the use of personal devices, especially on the appropriate use of smartwatches, which cannot be used to access the internet without the express permission of a member of staff to assist teaching and learning. Smartwatches cannot be worn in examinations, classroom assessments or tests.

- Mobile phones should not be used on the College site unless a member of staff has given their express permission to use them as part of teaching and learning.
- The College has no control over what students can access their own data plans on mobile phones.
- Regular audits and monitoring of usage will take place to ensure compliance.

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.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at College 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 in the digital / video images. See links to Information Security Policy.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow the College's policies concerning the sharing, distribution and publication of those images. Those images should only be taken on College equipment, the personal equipment of staff should not be used for such purposes. See links to Information Security Policy.
- 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 College into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, 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 or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published in the public domain.
- Students' work can only be published with the permission of the student and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that:

• The processing of personal data must be lawful and fair
• The purpose for collecting data must be specific, explicit and legitimate

• Data must be collected in a way that is adequate, relevant and not excessive
• Data must be kept for no longer than is necessary
• Data must be accurate and up-to-date
• Data must be processed in a way that ensures appropriate security and includes protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage
• Only transferred to others with adequate protection.

The College must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, 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, memory stick or any other removable media:

- Any sensitive or personal data must be encrypted and password protected
- Devices with sensitive or personal data must be password protected

- Sensitive and personal data must be securely deleted from the device, in line with College policy (below) once it has been transferred or its use is complete

The College has a Data Protection Policy, which covers this section in greater detail.

Related Policies
Safeguarding
Behaviour
Code of conduct
Grievance
Discipline
Complaints policy
Sex and relationships policy
Information security
Data protection
Privacy notices
IT acceptable use