Online Safety Policy

Together, we learn, love and grow with Jesus

Version	Autumn 26
To be reviewed	Autumn 27

Development/Monitoring/Review of this Policy

This online safety policy has been developed by a working group made up of:

- Headteacher – Mr Wilson
- Online Safety Coordinator – Mrs Jackson
- Staff – including teachers, support staff, technical staff (MGL)
- Computing and e-safety link governor – Tony Norris
- Safeguarding Deputy and Pastoral Lead – Mrs Ashurst
- Business manager – Mrs Shaw

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development/Monitoring/Review

The implementation of this online safety policy will be monitored by the:	*Mrs Jackson (computing lead)*
Monitoring will take place at regular intervals:	*Once per term*
The Board of Governors will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Once per 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:	*Autumn 2027*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of
    - students/pupils
    - parents/carers
    - staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the St. Jude's site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of St. Jude's, but is linked to membership of St. Jude's.

St. Jude's 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.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within St. Jude's:

Governors/Board of Directors

The computing link governor is responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Board (Mr Anthony Norris) has taken on the role of Online Safety Governor. He is also the Child Protection/Safeguarding Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator/computing lead
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting at Governors meeting

Headteacher

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead, Mrs Jackson.
- The Headteacher and the DHT (who is also the computing/online safety lead) are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (Appendix 1.1)
- The Headteacher is responsible for ensuring that the Online Safety Lead 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 Headteacher and Senior Leaders 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 to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading 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 taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff - MGL
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments. See appendix for log sheets.
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of Governors
- reports regularly to Senior Leadership Team

Network Manager/Technical staff

Those with technical responsibilities are responsible for ensuring:

- that St. Jude's technical infrastructure is secure and is not open to misuse or malicious attack

- that St. Jude's meets required online safety technical requirements and any Local Authority online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- 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 internet is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Online Safety Lead for investigation/action/sanction
- that monitoring software/systems are implemented and updated

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. Jude's online safety policy and practices and complete annual online safety training on the National College.
- they have read, understood and signed the staff acceptable use agreement (AUA)
- they report any suspected misuse or problem to the Headteacher/Online Safety Lead for investigation/action/sanction
- all digital communications with students/pupils/parents/carers 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
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- the use of AI is used in accordance with the school policy and inline with GDPR guidelines.
- 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
- in lessons where internet use is pre-planned pupils 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
- ensure that their use of personal mobile devices follow the agreed policy where they are only used in office areas, the Reception area and the staffroom and not used for anything connected to school.

Designated Safeguarding Lead

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
- online-bullying

Students/Pupils:

- are responsible for using St. Jude's digital technology systems in accordance with the student/pupil acceptable use agreement
- have a good understanding of 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. Y6 children who walk alone to school should be aware that if they take a mobile phone to school

they must give it to their teacher each morning when they arrive so it can be kept securely until the end of the school day. All pupils should also know and understand policies on the taking/use of images and on online-bullying.

- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that St. Jude's online safety policy covers their actions out of school, if related to their membership of the school

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. St. Jude's will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support St. Jude's 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 website, St. Jude's Facebook page and Class Dojo
- their children's personal devices in St. Jude's (these are allowed to be used in the Reception area only with the exception of Y6 children who walk to school alone. Their phones are collected by the Y6 staff in class each morning and kept securely until they are given out at home time again.)

Policy Statements

Education – Students/Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of St. Jude'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. Our online safety curriculum is Project Evolve. Teaching is targeted and all children are assessed prior to each unit of work so that teaching can be streamlined. It is broad, relevant and provides progression, with opportunities for creative activities. It will be provided in the following ways:

- A planned online safety curriculum will be provided as part of Computing/PHSE/RSE and will be regularly revisited. Children will be assessed regularly.
- Key online safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Pupils will 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.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will 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.
- Pupils will be helped to understand the need for the student/pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside St. Jude's.
- Staff will act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned. Pupils should be guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches in conjunction with our technical team, MGL and our filtering service, Smoothwall.
- Where pupils are allowed to freely search the internet, staff will 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 (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff from MGL 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/carers

Many parents and carers 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 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.

St. Jude's will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, Class Dojo
- Parents/carers evenings/online sessions
- 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-carers

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 on an annual basis. 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 as well as agreeing to adhere to our Acceptable User Agreement for staff, ensuring that they fully understand St. Jude's online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- This online safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The Online Safety Lead will provide advice/guidance/training to individuals as required.

Training – Governors

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

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation.
- Participation in training/information sessions for staff or parents.
- Annual online safety training

Technical – infrastructure/equipment, filtering and monitoring

St. Jude's will be responsible for ensuring that the network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

If you wish to see a more detailed Technical Security Template Policy, please ask.

- St. Jude's technical systems will be managed in ways that ensure that we meet recommended technical requirements.
- There will be regular reviews and audits of the safety and security of our technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to St. Jude's technical systems and devices.
- All users at Year 1 and above will be provided with a username and secure password by Mrs Hongkins (office staff) who will keep an up to date record of users and their usernames in a secure place. Users are responsible for the security of their username and password.
- The business manager, Mrs Shaw, 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 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. We work closely with MGL to deal with requests for filtering changes.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- St. Jude's has provided enhanced/differentiated user-level filtering.
- The computing lead, Mrs Jackson, receives daily reports from MGL via Smoothwall, monitoring and recording the activity of users on the school technical systems. Any inappropriate activity is recorded and investigated.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed. See appendix 1.1.
- 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 devices are protected by up to date virus software.
- In order to cater for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems guest logins are available.
- An agreed policy is in place in the Data Protection Policy regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Appendix 1.1

Name: _____Signed: _____Date:……..

Responding to incidents of misuse/Illegal incidents – flow chart

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, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.

