ST. JOSEPH'S CATHOLIC PRIMARY SCHOOL ALDERSHOT
A VOLUNTARY ACADEMY IN THE DIOCESE OF PORTSMOUTH
POLICY FOR E-SAFETY
(September 2020 - 2021)

VISION STATEMENT
As a Catholic family we welcome all and value Christ in everyone, whilst seeking the highest possible achievements.
The School's Vision and Mission Statements underpin this document.

At St Joseph's, we believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in our school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

At St Joseph's we aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- RSE
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996, the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The breath of issues classified within our online safety is considerable but can be categorised into three main areas of risk:

1. **Content**
    - Ignoring age ratings while playing online games (exposure to violence associated often with racist/foul language, addiction, in-app purchases).
    - Exposure to inappropriate content, including online pornography
    - Ignoring age restrictions on social networking websites e.g. Instagram, Fcaebook, YouTube, Snapchar, WhatsApp etc…
    - Data Breach
    - Hate sites, sites inciting radicalisation and/or extremism.
    - Content validation: how to check authenticity and accuracy of online content.
2. **Contact**
    - Grooming
    - Cyber-bullying in all forms
    - Identify theft and sharing passwords
3. **Conduct**
    - Privacy issues, including disclosure of personal information
    - Digital footprint and online reputation
    - Health and well-being (amount of time spent online)
    - Copyright
    - Inappropriate messaging

The policy also takes into account the National Curriculum computing programmes of study.

Role	Key Responsibilities
Headteacher	The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
Computing co-ordination and DSLs/Deputy DSLs	• Take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the schools e-safety policies and documents. • Promote an awareness and commitment to e-safety throughout the school. • Ensure e-safety education is embedded across the curriculum and the computing curriculum. • Updating and delivering staff training on online safety regularly. • Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material. • Ensuring that the school's computing systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly. • Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files • Ensuring that any online safety incidents are logged and dealt with appropriately in line with our child protection and safeguarding policy. • Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
All staff	• To read, understand and help promote the school's e-safety policies and guidance. • Agreeing and adhering to the school's computing systems and appropriate use of internet outlined in the Code of Conduct • Working with the DSL and deputy DSLs to ensure that any online safety incidents are logged and dealt with appropriately in line with our safeguarding and child protection policy. • Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
Governors	The Governors have overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governors will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL). The governor who oversees online safety is Jane Whittle All governors will: • Ensure that they have read and understand this policy • Agreeing and adhering to the school's computing systems and appropriate use of internet outlined in the Code of Conduct.
Parents/carers	• Notify a member of staff or the headteacher of any concerns or queries regarding this policy • Ensure their child is aware of acceptable use of the school's computing systems and internet. *Parents can seek further guidance on keeping children safe online from reading our safeguarding information and looking at the e-safety information on our parent portal.*

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

E-Safety is embedded throughout all curricular subjects especially in English, PE and PHSE/RSE and through a variety of enrichment activities e.g. anti-bullying and safeguarding week. The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website school website. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSLs.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Definition of Cyber Bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power (see also the school behaviour policy).

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes PSHE/RSE and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL/ deputies will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Acceptable use of the internet in school

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. The school system is "fire wall" protected so that inappropriate material cannot be accessed by pupils or staff.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the computing co-ordinator.

Work devices must be used solely for work activities.

How the school will respond to issues of misuse

Where a pupil misuses the school's computing systems or internet, we will follow the procedures set out in our schools behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's computing systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our safeguarding and child protection policy.

Monitoring arrangements

The DSL/ deputies logs behaviour and safeguarding issues related to online safety in-line with the schools safeguarding and child protection policy.

This policy will be reviewed annually by the computing co-ordinator and DSL/deputies. At every review, the policy will be shared with the governing board.

Links with other policies

This e-safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Whistleblowing Policy
- Staff disciplinary procedures
- Data protection policy (including GDPR)
- Staff Code of Conduct
- Complaints procedure

DATE OF APPROVAL:
Sept 2020

DATE OF REVIEW:
Sept 2021

Signed: Mrs D. McNeill
Headteacher

Dr. Campbell McCafferty CBE
Chair of Directors/Governors