

School Vision

In formulating and applying this policy, the Governing Body and Staff of our Catholic school seek to promote and implement in relevant ways the aims and intentions of the Mission Statement, *'Praise the Lord in Work, Play and Prayer'*, that has been agreed by the whole school community.

St Michael's Catholic Primary School embraces the challenge that Technology is now considered to be an essential part of modern life and it's a duty to provide pupils with quality technology as part of their learning.

This digital safe-guarding policy considers the use of both the fixed and mobile devices with an appropriate internet connection, PCs, laptops, webcams, digital video equipment, mobile phones, camera phones, personal digital assistants, gaming devices and portable media players. It will be revised to incorporate new and emerging technologies as they appear.

The purpose of technology use in school is to help deliver the whole school aims which is to offer a curriculum that is enhanced by integrating ICT across all subject areas, promoting enjoyment, a personal sense of fulfillment, achievement and the life skills that will help our children thrive in the 21st Century.

Equality and inclusion

The use of technology is a part of the statutory curriculum and a necessary means of delivering 21st Century teaching and learning for staff and pupils. Internet access is an entitlement for all. However, responsible and safe use must be at its core.

Technology in a changing world

Schools are part of a world where technology is integral to the way life is led in the 21st Century. Compared to even 5 years ago the technology available outside school is rapidly increasing. In line with the Gilbert review document *2020 Vision*, schools need to increasingly respond to:

- an ethnically and socially diverse society
- far greater access and reliance on technology as a means of conducting daily interactions and transactions
- a knowledge-based economy
- demanding employers, who are clear about the skills their businesses need and value
- complex pathways through education and training, requiring young people to make choices and reach decisions.

Why do learners need to be safe working with technology?

As the uses of online technological resources grow, so has the awareness of risks and potential dangers which arise for their use. This school aims to prepare its learners to be able to thrive and survive in this complex digital world. This policy outlines the safeguarding approach to achieve this.

Management of Digital Safeguarding

Roles and Responsibilities

- Headteacher

The Headteacher will ensure that the digital safeguarding policy is implemented and compliance with the policy monitored, and that the appropriate roles (see this section) and responsibilities of the school's digital safeguarding structure is in place. Ensure regular reports of the monitoring outcomes on digital safeguarding are reported to the governing body.

- Nominated Digital Safeguarding Coordinator

There is an identified digital safeguarding coordinator who is responsible for digital safeguarding developments in school and sharing of practice with staff and the wider community. This person will be in receipt of current training on the latest guidance and procedures and is the main contact for the Local Authority digital

safeguarding networks. All digital safeguarding incidents within the school need to be reported to this person. They need to keep the log of incidents and with the Headteacher make decisions about how to deal with reported incidents.

- Digital Safeguarding Governor

There is an identified digital safeguarding governor who monitors and liaises with the digital safeguarding coordinator and who will report to full governing board as appropriate.

- Digital safeguarding responsibility within subject and management roles

All staff with subject and management roles have a duty to incorporate digital safeguarding principles in their area of responsibility, deputising for any of the above roles where appropriate.

- Teachers

All staff understand the need for care and caution when using technology both for academic and social purposes and apply it to teaching and learning situations. They need to work to the agreed safe guarding guidelines. They have a "front line" monitoring and reporting role for incidents.

- Support Staff

As for teaching staff, however, given the nature of their role, learners may find it easier to disclose incidents to them. Support staff should be clear of the reporting procedures.

- School Council representatives

As a responsible member of their class the school council need to have digital safeguarding on their agenda as an item. These representatives could help to monitor at a learner level the appropriate use of technology within the school. They will be aware of to whom they should report digital safeguarding issues.

Procedures

- Are as defined in the School Child Protection and Safeguarding Policy.
- Incident log – All digital safeguarding incidents within the school must be reported to the nominated Digital Safeguarding coordinator. This nominated person will then keep the log of incidents and make decisions about how to deal with reported incidents.
- Monitoring - Monitoring will take place regularly as arranged by the Headteacher/Digital Safeguarding coordinator following LEA guidelines.
- Signing Agreements – Parents/carers will be required to sign consent for children to have their photograph taken and then published on the school learning platform. Procedures will be observed, as they are for signing consent for other aspects of school life.

Risks and acceptable Behaviours

- General use of the internet –Access to the Internet is gained via the Wolverhampton City Council intranet and this school uses appropriate web filtering of materials provided by the City Council. Children using the Internet will normally be working in the classroom, during lesson time and will be supervised by an adult. Pupils will be educated in taking responsibility for the information they access whilst connected to the Internet. Pupils will be informed that checks can be made on the information they are accessing and holding on the system. Pupils will be made aware that the writer of an email or author of a web page may not be the person they say they are. All pupils will be encouraged to tell a member of staff immediately should they encounter any material that makes them feel uncomfortable.
- Learning Platform - The learning platform will provide an important mechanism for communicating with parents, governors and the wider community. It is also a useful tool for providing samples of pupils work.
 - Pupils work will appear in an appropriate context and may not be copied without written permission.
 - Any personal or contact information for pupils will not be made available on the platform
 - Photographs of pupils are not encouraged however if it is felt necessary prior consent from parents is essential.
 - The Headteacher will delegate editorial responsibility to ensure that the content is accurate and quality of presentation is maintained.

- Pupils will be taught to publish for a wide range of audiences that might include Governors, parents and young children.
 - The platform is intended to promote the school and celebrate the work of pupils and staff.
 - All material must be the author's own work, or where permission to reproduce has been obtained it is clearly marked with the copyright owners name.
 - Pupils activity on the learning platform will be closely monitored. This monitoring will take place by the Wolverhampton e-services team.
- Data Protection and Security - The Data Protection Act came into force on 1 March 2000, and from 24 October 2001 covers the processing of paper records. The Act is not optional, every school must comply with the provisions of the Act; the school is also responsible if a person suffers harm or damage due to the infringement of the Act.
 - School websites are an important link to the community, and a means of promoting school activities and events. This however also means that information on the website has the capacity of being passed outside of the LEA and as such stringent rules apply.
In accordance with the Act, this school will:
 - Obtain the consent of parents prior to publishing any child's information on a web page.
 - Only publish photographs of children with prior consent of parents.
 - Seek advice from the City Council when required.
 - Social networking/cyberbullying – Access to social network sites is blocked through the use of web filtering provided by the City Council. Children will have lessons focused on e-safety throughout the year.
 - Mobile phones/technology – The use of mobile phones in school is strictly prohibited and children are made aware that mobile phones that are required for after school must be left in the school office at the start of the school day. Staff must not use their own mobile phones to take photographs of children.

Physical and technical security

- Firewall and Filtering provision – Firewalls, Filtering and other security measures are provided for St Michael's Catholic Primary School by the City Council
- Antivirus software – All school computers and laptops include Kaspersky virus scanning software which is designed to intercept any viruses in email attachments and files downloaded from the Internet.
- Security marking - All ICT equipment in school have appropriate Wolverhampton City Council security markings.

Monitoring and Review

The policy will be reviewed on annual basis.

Signed: (Chair of Governors)

Date:

Appendices:

- E-Safety Strategy
- Acceptable Users Policies
- Digital Technology Parental Agreement