



Saint Michael Catholic Primary School

Internet Safety Policy

Mission Statement:

Excellence • Enrichment • Enjoyment

Agreed: September 2026

Date for review: July 2027

Aim of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors and community users) who have access to and are users of school IT systems.

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 school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other internet safety incidents covered by this policy, which may take place outside of the school but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy).

The school 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 internet behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the internet safety roles and responsibilities of individuals and groups within St Michael Catholic Primary School & Nursery Governors.

Governors are responsible for the approval of the Internet Safety Policy and for reviewing the effectiveness of the policy.

- The Headteacher has a duty of care for ensuring the safety (including internet safety) of members of the school community, though the day to day responsibility for internet safety will be delegated to the Computing Leader
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious internet safety allegation being made against a member of staff. (see flow chart on dealing with internet safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / other relevant body disciplinary procedures).
- The Headteacher is responsible for ensuring that the Computing Leader and other relevant staff receive suitable training to enable them to carry out their internet safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal internet safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

Child Protection / Safeguarding Designated Person should be trained in internet 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

Pupils:

- are responsible for using the school digital technology systems
- 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. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good internet safety practice when using digital technologies out of school and realise that the school's Internet 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. The school will take every opportunity to help parents understand these issues. Parents and carers will be encouraged to support the school in promoting good internet 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
- their children's personal devices in the school (where this is allowed)

Policy Statements

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 internet safety is therefore an essential part of the school's internet provision.

Children and young people need the help and support of the school to recognise and avoid internet risks and build their resilience.

Internet safety should be a focus in all areas of the curriculum and staff should reinforce internet safety messages across the curriculum. The internet safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned internet safety curriculum should be provided as part of Computing / PSHCE / other lessons and should be regularly revisited
- Key internet safety messages should be reinforced as part of a planned programme of assemblies and lesson activities
- Pupils 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.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- 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 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – parents / carers

Many parents and carers have only a limited understanding of internet 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 carers through:

- Curriculum activities
- Letters & newsletters,
- Parents Workshops
- Reference to the relevant web sites / publications e.g. www.saferinternet.org.uk/

<http://www.childnet.com/parents-and-carers>

<http://net-aware.co.uk>

Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff.

Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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 limiting access to personal information:

Clear reporting guidance, including responsibilities, procedures and sanctions
Risk assessment, including legal risk

CYBERBULLYING

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated.

Full details are set out in the school's policy on anti-bullying and behaviour.

The school will follow procedures in place to support anyone in the school community affected by cyberbullying.

All incidents of cyberbullying reported to the school will be recorded.

The school will follow procedures to investigate incidents or allegations of cyberbullying.

Pupils, staff and parents and carers will be advised to keep a record of the bullying as evidence.

The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.

Pupils, staff and parents and carers will be required to work with the school to support the approach to cyberbullying and the school's internet ethos.

Sanctions for those involved in cyberbullying will follow those for other bullying incidents and may include:

I. The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.

II. Internet access may be suspended at the school for a period of time.

III. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy.

IV. Parent and carers of pupils will be informed.

V. The police will be contacted if a criminal offence is suspected.