St Michael's Church of England VA Primary and Nursery School

Dream, Believe, Achieve

We are a school, rooted and inspired by Christian values, which nurtures children to achieve infinitely more than we might ask or they may dream; empowering them so they can flourish as confident citizens now and in the future.

ONLINE SAFETY POLICY

Policy Consultation & Review

This policy is referred to on our website and is available on request from the school office. We also inform parents and carers about this policy when their children join our school and through our school newsletter. This policy is part of the School's statutory Safeguarding Policy. Any issues and concerns with online safety will follow the school's safeguarding and child protection processes.

This policy is overseen by the Designated Safeguarding Lead (DSL) and will be reviewed bi-annually by the Governing Body.

Last reviewed on:	December 2021
Next review due by:	December 2023

Related policies and documents

Consent forms
Data Protection Policy
ICT Code of Conduct
Staff Code of Conduct

1. Introduction and Overview

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at St Michael's School with respect to the use of technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with technology and to monitor their own standards and practice.
- Set clear expectations of behaviour and codes of practice relevant to responsible use of technologies for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

- Exposure to inappropriate online content

- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content
- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords
- Aggressive behaviour (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of St Michael's School community (including staff, pupils, volunteers, parents and carers, visitors, community users) who have access to and are users of school technology, both in and out of St Michael's School.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- It is posted on the school website and staffroom.
- It is part of school induction pack for new staff, including information and guidance where appropriate.
- All staff must read and sign the Staff Code of Conduct and ICT Code of Conduct before using any school technology resource.
- There will be regular updates and training on online safety for all staff.
- The ICT Code of Conduct is discussed with staff at the start of each year.
- Parents and carers are made aware of the policy and ICT Code of Conduct when children on come to this school.

Handling Concerns

The school will take all reasonable precautions to ensure online safety is in line with current guidance from the Department for Education (DfE)

Staff and pupils are given information about infringements in use and possible sanctions.

Designated Safeguarding Lead (DSL) acts as first point of contact for any safeguarding incident whether involving technologies or not

Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the concern is referred to the Chair of Governors.

2. Education and Curriculum

Online safety is covered as part of the Computing curriculum and PSHE. It is always tailored to children's age and experience.
Children are taught about acceptable use in line with their age. Parents agree to support this when their child joins the school. (See consent forms)

We ensure staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright.

We ensure that staff understand issues around plagiarism, how to check copyright and also know that they must respect and acknowledge copyright and intellectual property rights.

Staff and governor training
Regular up to date training is delivered to staff on online safety issues.

All staff are provided, as part of the induction process, with information and guidance on the online safety and must agree to the ICT and Staff Codes of Conduct.

Parent/Carer awareness
We provide up to date information for parents and carers for online safety via the school website.

We remind parents and carers regularly about online safety issues and signpost them to advice and training whenever it is available.

We ask all new parents to read and sign the following agreements when their children begin school here.

- Acceptable Use Policy (Internet Use)
- Consent for Internet Access
- Consent for Web Publication of Work and Photographs
- Use of digital and video images

And reference to online safety is made in the Home/School agreement.

3. Incident management

When dealing with online safety incidents we will look for support from other agencies, i.e. the Local Authority, UK Safer Internet Centre helpline, CEOP, the police, Internet Watch Foundation.

We will monitor and report on incidents, and we will involve parents or carers when following up. The police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

We will immediately refer any suspected illegal material to the appropriate authorities, as listed above.

4. Managing IT and Communication System

We follow guidelines issued by the Department for Education to ensure that we comply with minimum requirements for filtered broadband provision.

The Education Network (NEN) has produced a school e-security checklist, setting out 20 e-security controls that, if implemented effectively, will help to ensure that school networks are kept secure and protected from internal and external threats.

We use this to make sure that e-security is tight at this school.

5. E-mail

Staff are provided with an email account for their professional use, e.g. nsix.org.uk and insists that personal email should be through a separate, private account.

We also use anonymous e-mail addresses, for example head@, office@.

We reserve the right to block personal email accounts.

We will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.

We ensure that email accounts are maintained and up to date.

Staff know that they must never use email to transfer staff or pupil personal data unless it is protected with secure encryption. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

Pupils are not given email addresses at this school.

6. School website

The school website complies with statutory DfE requirements

Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.

Photographs of pupils published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

7. Social networking

Staff agree to keep professional and private communication separate.

Teachers and support staff are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to children or their parents, but to use the schools' preferred system for such communications.

The use of any school approved social networking will adhere to the ICT Code of Conduct.

Children are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.

Parents/carers are reminded about social networking risks and protocols through the ICT Code of Conduct/AUP and additional communications materials when required.

8. Data Security

We use guidance from the Information Commissioner's Office to ensure that we comply with our responsibilities to information rights in school. (see also Data Protection Policy)

9. Equipment and Digital Content

We gain parental/carer permission for use of digital photographs or video involving their child as part of the consent form when their daughter/son joins the school.

We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials or DVDs.

Staff sign the school's ICT Code of Conduct/AUP and this includes a clause on the use of personal mobile phones and other digital personal equipment.

If specific pupil photos (not group photos) are used on the school web site, in any prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use.