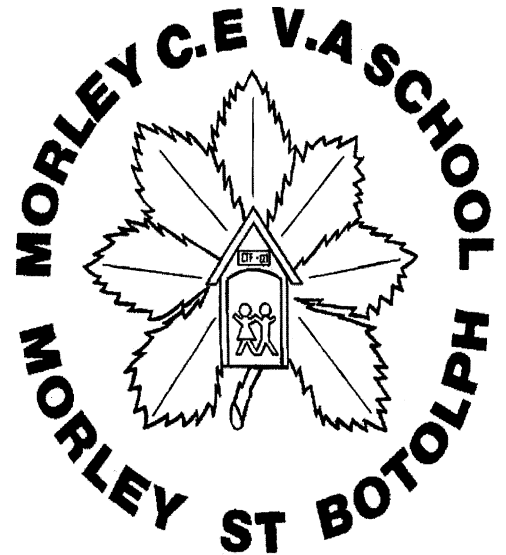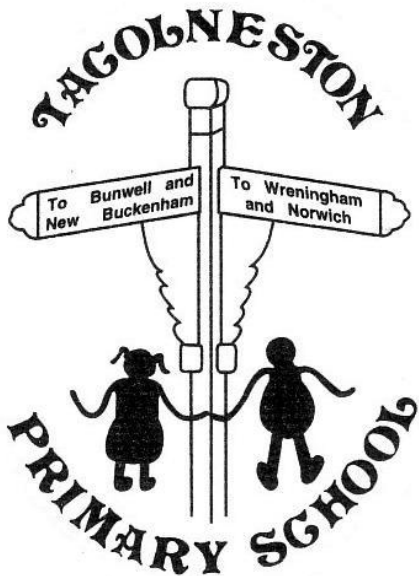# Tacolneston & Morley CE VA Primary Schools Federation

E-Safety Policy

All policies at Tacolneston & Morley CE VA Primary Schools Federation should be taken as part of the overall strategy of the school and implemented within the context of our Safeguarding Policy and our vision, aims and values as Church of England Schools.

Agreed: Autumn 2019

Head Teacher: Governor:

Review: Autumn 2020

Tacolneston & Morley CE VA Primary Schools Federation

E-SAFETY POLICY

1.1 Writing and reviewing the e-safety policy

The e-Safety Policy is part of safeguarding/school development plan and relates to other policies including those for ICT, bullying and for safeguarding.

- The Federation will identify a member of staff who has an overview of Online Safety, this is the Designated Safeguarding Lead (DSL).
- Our E-Safety Policy has been written by the Federation, based on best practice; government guidance and General Data Protection Regulations. It has been agreed by staff and approved by governors.
- The E-Safety Policy and its implementation will be reviewed annually.

1.2 Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Morley and Tacolneston Schools with respect to the use of technologies.
- Safeguard and protect the children; staff and governors.
- Assist governors and school staff working with children to work safely and responsibly with technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or 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
- 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 children.

1.3 Scope

This policy applies to all members of the Morley and Tacolneston School community (including governors; staff; students; pupils; volunteers; parents; carers; visitors; and community users) who have access to and are users of school technologies, both in and out of the schools.

Refer also to our Safeguarding Policy; Data Handling Policy; Behaviour Policy; Internet, Social Networking and Email Use Policy and Photographs Policy.

2. Teaching and learning

2.1 Why Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet use will enhance learning by personalising the curriculum for individuals, and enabling access to a much broader range of digital information, which is topical and up-to-date.

2.2 Internet use and learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

2.3 Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law and General Data Protection Regulations (GDPR)
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content

3. Managing Internet Access

3.1 Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.

3.2 E-mail

- Pupils, staff and governors may only use approved e-mail accounts on the school system.
- Pupils must immediately tell an adult if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.
- Provides staff with an email account for their professional use, e.g. nsix.org.uk and makes clear personal email should be through a separate account
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.
- If e-mailing about a child, their name should not appear in the subject heading and initials should be used.

3.3 Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.4 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully.
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Written permission from adults will be obtained before their names, photographs or images of themselves are published
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

3.5 Social networking and personal publishing

- The school will block/filter access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and staff will be advised on the safe use of social network spaces
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

3.6 Managing filtering

- The school will work with the Data Protection Officer (Data Protection Education); Norfolk Children's Services and guidelines issued by the Department for Education (DfE) to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Head Teacher (Designated Safeguarding Leader and Data Controller).
- Staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils should not bring mobile phones to school but where a phone is necessary for a specific and previously agreed (with the Head Teacher) reason, it will be stored in the school office during formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required.

3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the latest General Data Protection Regulations.

Tacolneston & Morley CE VA Primary Schools Federation

4. Policy Decisions

4.1 Authorising Internet access

- All adults must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- At Key Stage 2, pupils must agree to comply with the Responsible Internet Use statement before being granted Internet access.
- Parents will be asked to sign and return a consent form.

4.2 Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material in line with current guidance from the Department for Education (DfE). However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Norfolk County Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will regularly audit computing provision to establish if the e-safety policy is adequate and that its implementation is effective.

4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff/Designated Safeguarding Lead (DSL).
- Any complaint about staff misuse must be referred to the headteacher or senior member of staff.
- Complaints of a safeguarding nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

4.4 Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety policy.

5. Communications Policy

5.1 Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils

5.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- All staff must read and sign the 'Staff Code of Conduct' before using any school technology resource
- Regular updates and training on online safety for all staff will be provided, including any revisions to the policy

5.3 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in the school brochure and on the school Web site.
- Parents and carers will from time to time be provided with additional information on E-safety.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.