

---

# Nacton Church of England Primary School

Nacton Village  
Ipswich  
IP10 0EU

(01473) 659370

---

## Online Safety Policy

Version 8

Chair of Governors: Mrs Melanie Munday

Signed: \_\_\_\_\_

Chair of working group: Mr Owen Wheeler

Signed: \_\_\_\_\_

Date authorised: \_\_\_\_\_

Approval minuted: 21 June 2018

Date of next review: Summer Term 2019

---

## **1 Writing and reviewing the online safety policy**

The online safety Policy relates to other policies including those for Computing, bullying and for safeguarding.

- The school will appoint an online safety Coordinator who will work in co-operation with the Senior Designated Person (safeguarding).
- Our online safety Policy has been written by the school, building on the Kent online safety Policy and government guidance. It has been agreed by senior management and approved by governors.
- The policy is reviewed annually.

## **2 Teaching and learning**

### **2.1 Why the Internet and digital communications are important**

As part of the school's Computing programme, we offer pupils supervised access to the Internet.

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.

Our aim when using the Internet is to ensure that children can use this educational opportunity safely and confidently.

### **2.2 Internet use will enhance 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.
- Pupils will be shown how to publish and present information to a wider audience.

### **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.
- Pupils will be taught the importance of crosschecking information before accepting its accuracy.

- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP (Child Exploitation and Online Protection Centre) Report Abuse icon or Hector Protector.

### **3 Managing Internet Access**

#### **3.1 Information system security**

- School IT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority and IT provider.

#### **3.2 Published content and the school web site**

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

#### **3.3 Publishing pupil's images and work**

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused, with the use of group photographs rather than full-face photos of individual children.
- Pupils' full names will not be used anywhere on a school Web site or other on-line space, 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 and Twitter.
- Work can only be published with the permission of the pupil and parents/carers.
- Pupil image file names will not refer to the pupil by name.
- Parents/carers should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

#### **3.4 Social networking and personal publishing**

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Pupils will be advised never to give out personal details of any kind that may identify them, their friends or their location.

- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

### **3.5 Managing filtering**

- The school will work with the MAT and follow Department for Education guidance to ensure systems to protect pupils are reviewed and improved (filtering uses the E2BN Protex product via a central proxy; children normally use the Primary school settings).
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the online safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

### **3.6 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.
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- Staff will be issued with a school iPad where photos are required
- The use of tablet computers in classrooms is monitored and the Internet access is via the school filtering system.

### **3.7 Protecting personal data**

- Personal data will be recorded, processed, transferred and made available according to the requirements of the General Data Protection Regulation (GDPR) and the *Data Protection Act 2018*.

## **4 Policy Decisions**

### **4.1 Authorizing Internet access**

- All staff must read the acceptable use policy for ICT before using any school ICT resource.

- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Any person not directly employed by the school will be asked to sign an acceptable use of school ICT resources before being allowed to access the Internet from the school site.

#### **4.2 Assessing risks**

- The school will take all reasonable precautions to prevent access to inappropriate material. 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 computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate and effective.

#### **4.3 Handling online safety complaints**

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures.
- Pupils and parents/carers will be informed of the complaints procedure (see schools complaints policy)
- Pupils and parents/carers will be informed of consequences for pupils misusing the Internet.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

#### **4.4 Community use of the Internet**

- The school will liaise with local organizations and parents to establish a common approach to online safety.

## **5 Communications Policy**

### **5.1 Introducing the online safety policy to pupils**

- Online safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- Pupils will sign a contract to confirm they will follow the rules for Internet use and that they understand the consequences.
- A programme of training in online safety will be developed, including the materials from CEOP (Child Exploitation and Online Protection Centre).
- Online safety training will be embedded within the ICT scheme of work and the Personal Social and Health Education (PSHE) curriculum.

### **5.2 Staff and the online safety policy**

- All staff will be given the School online safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

### **5.3 Enlisting parents' and carers' support**

- Parents and carers' attention will be drawn to the School online safety Policy in newsletters, the school brochure and on the school Web site.
- The school will maintain a list of online safety resources for parents/carers.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.

## 6 Document History

Version	Date	Comments
A	January 2009	Initial draft, based on Kent County Council template (© KCC, used with permission), with revisions.
1	16/06/2010	Issued with changes agreed at Spring FGB meeting.
2	15/06/2011	Minor revisions.
3.1	20/06/2012	Minor revisions. Text of version 3 approved, but counter-signature changed from Curriculum Group to Management Committee to reflect sign-off at FGB; marked as version 3.1, no other changes.
4	18/06/2014	Noted filtering uses E2BN Protex service. No other changes.
5	18/06/2015	No changes.
6	30/06/2016	Updates for terminology and learning platform.
7	12/06/2017	Title changed E safety changed to online safety throughout document and ICT changed to Computing. Removed line regarding finance committee updating policy. 3.1 ICT changed to IT, included IT provider 3.2 Removed 3.5 Edited to reflect current practice 3.6 LA changed to MAT 3.7 Removed 3.8 Children's phone camera use removed and games console use removed. Teachers provided with an iPad. 4.1 Internet use consent form removed. 5.1 Reference to Appendix 2 removed.
8	21/06/2017	Added reference to the GDPR and DPA 2018. Added reference to Twitter