St John Vianney
Catholic Primary School

"Seeking Growth Together"

E-Safety and Internet Access Policy

Date Reviewed: September 2017
Reviewed by: A. Smith / C. Walsh
Approved by Headteacher
Date of next review: September 2018

Contents

Writing and reviewing the E-safety policy 3
Teaching and Learning 3
Why Internet use is important 3
Internet use will enhance learning 3
Pupils will be taught how to evaluate Internet content 3
Managing Internet Access 4
Information system security 4
E-mail 4
Published content and the school web site 4
Publishing pupil's images and work 4
Social networking and personal publishing 4
Cyberbullying 5
Managing filtering 5
Managing videoconferencing 5
Managing emerging technologies 5
Protecting personal data 5
Policy Decisions 6
Authorising Internet access 6
Assessing risks 6
Handling e-safety complaints 7
Prevent Policy 7
Communications Policy 8
Introducing the e-safety policy to pupils 8
Staff and the e-Safety policy 8
Enlisting parents' support 8
Incident Reporting 8
Appendices 9
Appendix A – E-Safety Incident Report Form 9
Appendix B – E-Safety Rules (KS1) 11
Appendix C – E-Safety Rules (KS2) 12

Writing and reviewing the E-safety policy

The E-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying, child protection, acceptable usage and for Prevent.

The school's ICT Co-ordinator will also act as E-Safety Coordinator.

Our e-Safety Policy has been written by the school, building on the government and CEOP e-Safety guidelines. It has been agreed by senior management and approved by governors. The E-Safety Policy and its implementation will be reviewed annually.

This policy should be read in conjunction with the prevent policy, behaviour policy and acceptable usage policies. We pay due regard to the Prevent Duty 2015.

Teaching and Learning

Why Internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children 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

The school Internet access is designed expressly for pupil use and includes 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 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 should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

School ICT systems capacity and security will be reviewed regularly.

Virus protection is updated regularly. Content filtering services will be updated from centrally recognised databases conforming to current standards and requirements.

E-mail

Pupils may only use approved e-mail accounts on the school system and email usage should be supervised and monitored by a staff member.

The pupil email system does not allow emails from or to external domains and therefore pupils can send and receive emails from/to other pupils or staff within school.

Pupil emails are checked by their class teacher before they appear in their inbox.

Pupils must immediately tell a teacher 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.

The forwarding of chain letters is not permitted.

Published content and the school web site

School is responsible for ensuring and published items meet requirements such as following the 'What maintained schools must publish online' document.

Staff or pupils' personal information will not be published.

The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

In the modern changing world the school wants to create an audience for the children and so will utilise multi-media appropriate web sites such as Vimeo, Animoto, etc. The school will publish video, photographic and audio recordings of the children. Pupils' full names will not be associated with any of the recordings. Parents and guardians will be given the opportunity to opt out and not have their child's recordings published.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Social networking and personal publishing

The school will block/filter/monitor access to social networking sites.

Pupils will be advised never to give out personal details of any kind that may identify them or their location.

Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils (pupils aged 12 and under).

Cyberbullying

Cyberbullying, along with all other forms of bullying, of any member of St John Vianney Catholic Primary School community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.

Managing filtering

The school will work in partnership with parents, Blackpool Safeguarding Board, the DfE and CEOP's guidelines to make use of the schools' web filtering system to ensure systems to protect pupils are reviewed and improved.
If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Coordinator.
Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

IMPORTANT NOTE: It should be noted that the main aim of content filtering is to MINIMISE THE RISK OF USERS ACCESSING INAPPROPRIATE MATERIAL ON THE INTERNET. Whilst the content filtering provision will significantly contribute towards this, it should NOT be viewed as a complete solution that will block all inappropriate material and therefore should be underpinned with good practice at home and at school.

Managing videoconferencing

Currently the unsupervised use of video conferencing including services and applications such as FaceTime and Skype is not permitted at any time.
Videoconferencing will be appropriately supervised for the pupils' age.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before implementation where appropriate.
Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

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

All staff are Data Protection trained as part of their introduction to working at St John Vianney Catholic Primary School.

Please also see the school's Data Protection Policy.

Policy Decisions

Authorising Internet access

All staff and visitors must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.

Assessing risks

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. St John Vianney Catholic Primary School cannot accept liability for the material accessed, or any consequences of Internet access. Methods to identify, assess and minimise risks will be reviewed regularly.
The Headteacher will ensure that the Internet policy is implemented and compliance with the policy monitored. The following table outlines some of the potential risks:

Area of risk	**Examples of risk**
Commerce: Pupils need to be taught to identify potential risks when using commercial sites.	Advertising Privacy of information (phishing, identity fraud) Invasive software (e.g. virus, trojan, spyware) Online gambling Premium rate sites
Content: Pupils need to be taught that not all content is appropriate or from a reliable source.	Illegal materials Inaccurate / bias materials Inappropriate materials Copyright and plagiarism User generated content (e.g. YouTube, sexting)
Contact: Pupils need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	Grooming Cyberbullying Contact inappropriate emails / blogs / instant messaging Encouraging inappropriate contact

Handling e-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 procedures.
Pupils and parents will be informed of the complaints procedure.

Prevent Policy

When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the school safeguarding policy. Please see the school's Prevent Policy for further information.

Communications Policy

Introducing the e-safety policy to pupils

E-safety rules will be displayed on the school's website. E-safety will be discussed with pupils each half-term as part of the ICT and Computing Curriculum.
Pupils will be informed that network and Internet use will be monitored.

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.

Enlisting parents' support

Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

Incident Reporting

Details of all E-safety incidents are to be recorded using the form (see Appendix A) and forwarded to the E-safety co-ordinator. The incident logs will be monitored termly by the E-safety co-ordinator and SMT.

Appendices

Appendix A – E-Safety Incident Report Form

St John Vianney E-Safety Incident Report Form

This form should be kept on file in the ICT Technician's room and a copy emailed to Mr Walsh (ICT Co-ordinator) chris.walsh@st-john-vianney.blackpool.sch.uk

Details of Incident

Date of incident: **Time:**

Name of person reporting incident:

If not reported, how was the incident identified?

Where did the incident occur?

- ☐ In school
- ☐ Outside school

Who was involved in the incident?

- ☐ Child
- ☐ Staff Member
- ☐ Other (please specify)

Type of incident:

- ☐ Bullying or harassment (cyber bullying)
- ☐ Deliberately bypassing security or access
- ☐ Hacking or virus propagation
- ☐ Racist, sexist, homophobic religious hate material
- ☐ Terrorist material
- ☐ Drug/bomb making material
- ☐ Child abuse / concern images
- ☐ Pornographic material
- ☐ Other

Description of the incident

Nature of incident

- ☐ Deliberate access
- ☐ Accidental access

Did the incident involve material being:

☐ Created ☐ Viewed ☐ Printed ☐ Shown to others ☐ Transmitted to others ☐ Distributed

Could the incident be considered as:

☐ Harassment ☐ Grooming ☐ Cyber bullying ☐ Breach of AUP

Action taken

- Staff
    - Incident reports to head teacher / senior management
    - Advice sought from Safeguarding and Social Care
    - Referral made to Safeguarding and Social Care
    - Incident reported to Police
    - Incident reported to Internet Watch Foundation
    - Incident reported to IT
    - Disciplinary action to be taken
    - E-safety policy to be reviewed / amended
- Child / Pupil
    - Incident reported to head teacher / senior management
    - Advice sought from Safeguarding and Social Care
    - Referral made to Safeguarding and Social Care
    - Incident reported to Police
    - Incident reported to social networking site
    - Incident reported to IT
    - Child's parents informed
    - Disciplinary action to be taken
    - Child / pupil debriefed
    - E-safety policy to be reviewed / amended

Details of any specific action taken (I.e. Blocking of website / removal of equipment)

Outcome of incident

Appendix B – E-Safety Rules (KS1)

THINK! – Then Click

KS1 – e-Safety Rules for the School

These rules help us to stay safe on the Internet:

- We only use the internet when an adult is with us
- We can click on the buttons or links when we know what they do.
- We can search the Internet with an adult.
- We always ask if we get lost on the Internet.
- We can send and open emails together.
- We can write polite and friendly emails to people that we know.

Appendix C – E-Safety Rules (KS2)

THINK! – Then Click

KS2 – e-Safety Rules for the School

At St John Vianney Catholic Primary School we;

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.
- We do not use mobile phones in school.