



Our Lady of the Assumption Catholic Primary School



Online Safety Policy

Our Mission Statement:

'Love One Another As I Have Loved You' (John 13:33-34)

Agreed by Governors on 7th June 2017 to be implemented in September 2017

Signed:  Chair of Governors

Review date: June 2019

Safeguarding Statement:

'Our Lady of the Assumption Catholic Primary School is committed to safeguarding and promoting the safety and welfare of all children and expects all staff, parents and volunteers to share this commitment.'

Our Vision

As a Catholic school that puts Christ at the centre, we are committed to encouraging everyone to 'Be the Best They Can Be'

Values and Ethos

We believe that everyone is made in the image and likeness of God and we value the equality of all, reject discrimination of any kind, and welcome the diversity of different cultures.

INTRODUCTION

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 students 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 will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught about acceptable 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 IT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Head Teacher and IT Technician

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- 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-mails 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

- 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.

Publishing pupil's images and work

- Photographs/Film that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Website or in class Dojos , particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs/film of pupils are published on the school Web site.
- Pupil's work can only be published with the permission of the pupil and parents.
- There may be occasions when the children are in a public place e.g City Centre / Sports event etc and a photograph may appear in the local press. The school cannot legislate against such pictures being taken or published as they would not be given prior knowledge of publication.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which 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.

Managing filtering

- The school will work with the Local Authority and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Senior Leadership Team.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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.
- 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.

Policy Decisions

Authorising Internet access

- All staff 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, access to the Internet will be independent, but with an adult present in the room.
- Parents will be asked to sign and return a consent form.

Assessing risks

- 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.
- The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The school will audit IT provision to establish if the Online Safety policy is adequate and that its implementation is effective.

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

Communications Policy

Introducing the Online Safety policy to pupils

- Online 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.

Staff and the Online Safety Policy

- All staff will be given the School Online 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.
- Staff should not remain logged on to a machine or disclose details of passwords.

Enlisting parents' support

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

Failure to Comply

Failure to comply in any way with this policy will be considered a serious risk to health and safety and all incidents of non-compliance will be investigated by a senior member of staff.

Appendices:

- 1. Online Safety Rules for KS1**
- 2. Online Safety Rules for KS2**
- 3. Acceptable Use Agreement for staff**
- 4. Acceptable Use Agreement for EYFS/KS1 children**
- 5. Acceptable Use Agreement for KS2 children**



*Our Lady of the Assumption
Catholic Primary School*



Online Safety Rules for EYFS / KS1

Think then Click

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.





*Our Lady of the Assumption
Catholic Primary School*



Online Safety Rules for KS2

Think then Click

Online Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only search for websites that the teacher has suggested.
- 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 never give out personal information or passwords.
- We do not try to use Internet chat rooms.



Our Lady of the Assumption Catholic Primary School



IT Acceptable Use Agreement for Staff

To ensure that members of staff are fully aware of their professional responsibilities when using school information systems they are required to sign this code of conduct.

- I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will only install/download any software or hardware if it is beneficial to the children's learning
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Headteacher.
- I will promote online safety with children in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will take responsibility for the security of devices given to me.

Virus Control:

Devices must have an Anti-Virus software package installed. Users are not to alter the configuration of this package. This package has been installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files.

If a virus is discovered the following actions must be carried out:

- Disconnect immediately from the network
- Turn the device off
- Inform the IT Technician

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. This will be achieved through using IMPERO SOFTWARE.

I have read, understood and accept the Acceptable Use Agreement for staff

Staff signature:

Date:

Approved/Authorised by Name (in Caps):

Signature:

Date:



*Our Lady of the Assumption
Catholic Primary School*



Acceptable Use Agreement for FKS/KS1

I want to feel safe all the time.

I agree that I will:

- always keep my passwords safe
- only open pages which my teacher has said are OK
- tell my teacher if anything makes me feel scared or uncomfortable
- talk to my teacher before using anything on the internet

Class Signatures:



*Our Lady of the Assumption
Catholic Primary School*



Acceptable Use Agreement for KS2

*When I am using the computer or other technologies,
I want to feel safe all the time.*

In school, I agree that I will:

- always keep my passwords safe
- only visit sites which have been approved by my teacher or are appropriate to my work at the time
- tell a responsible adult straight away if anything makes me feel unsafe

Outside of school, I will be a responsible IT citizen and I agree that I will:

- make sure all messages I send are respectful
- not accept friend requests online from people that I do not know.
- try to make a friend of someone I don't know.
- show a responsible adult if I get a nasty message or get sent anything that makes me feel uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a known friend
- talk to a responsible adult before joining chat rooms or networking sites
- always keep my personal details private. (My name, family information, journey to school, my pets and hobbies are all examples of personal details)
- only communicate people I know or those approved by a responsible adult
- always check with my parents before I show photographs of myself
- never meet an online friend without taking a responsible adult that I know with me

Class Signatures: