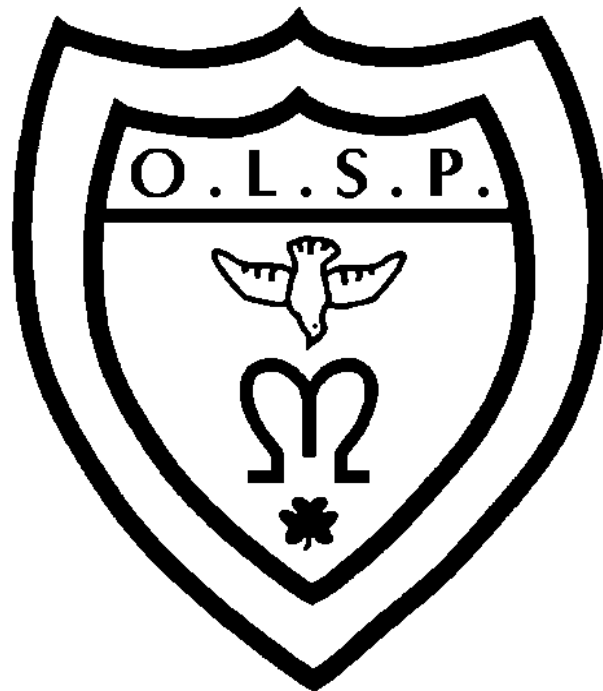


**Our Lady and St Patrick's  
Roman Catholic  
Nursery and Primary School**



***A family of schools working together***  
**E-Safety Policy**

**Reviewed By: Resources/FGB**

# Our Lady & St Patrick's Catholic Primary

## School E-Safety Policy

### Rationale

- New technologies have become integral to the lives of children and young people in today's society, and for the 21<sup>st</sup> century, both within schools and in their lives outside school.
- The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.
- The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.
- Unfortunately, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:
  - Access to illegal, harmful or inappropriate images, video games or other content
  - Unauthorised access to / loss of / sharing of personal information
  - The risk of being subject to grooming by those with whom they make contact with on the internet
  - The sharing / distribution of personal images without an individual's consent or knowledge
  - Inappropriate communication / contact with others, including strangers,
  - Sexting
  - Implications of Geolocation
  - Cyber-bullying
  - An inability to evaluate the quality, accuracy and relevance of information on the internet
  - Plagiarism and copyright infringement
  - Illegal downloading of music or video files
  - The potential for excessive use which may impact on the social and emotional development and learning of the young person

***Many of these risks reflect situations in the “offline world” and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. anti-bullying, child protection and data protection policies).***

### Development / Monitoring / Review of this Policy

- This e-safety policy has been developed by the Designated Person for Child Protection, the ICT Subject Leader and governors.
- It is to be reviewed annually by the ICT Subject Leader and Designated Person for Child Protection and Resources committee.
- The implementation of the policy will be monitored by the Designated Person for Child Protection.

## Scope

This policy applies to all members of the school community including staff, pupils, visitors, governors and community users who have access to, and are users of, the school ICT systems both in and out of school.

## Technical/infrastructure/equipment

- All users will have clearly defined access rights to school ICT systems.
- Users will be made responsible for the security of their username and password, and must not allow other users to access the systems using their log on details
- Internet content (particularly images) is filtered by the SWGFL systems.
- The system is maintained by an external IT supplier under the guidance of the Assistant Head.
- An appropriate system is in place (to be described) for users to report any actual / potential e-safety incident on the Network.
- An agreed policy is in place regarding the downloading of executable files by users and the installation of software.
- USB devices may only be used on the Network after having been virus checked.

## Curriculum/Pupil Use

- Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision.
- A planned e-safety programme will be provided as part of ICT / EPR / other lessons and will be regularly revisited by the pupils to learn the risks of e-communication (personal details, viruses, phishing, cyber-bullying, Internet risks, copyright, longevity of posted information/images etc.)
- Key e-safety messages are reinforced in assemblies.
- E-safety week is taught every half term to ensure new resources and trends are discussed and kept up to date.
- Rules for use of ICT systems / internet are posted in rooms
- Pupils may only use computers/digital resources under the supervision of a member of staff – the adult may not necessarily be standing over them and therefore must understand their own responsibilities to use the ICT equipment appropriately.
- KS2 pupils may only use the Internet to search for resources to use in school-work.
- The use of websites for other purposes i.e. to play games is only permitted by prior agreement with a member of staff. Lunch Clubs may only access approved sites.
- Pupils must ask for permission before searching using Google Images.
- **Pupils not using computers responsibly will be denied freedom of access.**
- Pupils must be advised as to the social, health and emotional impact of the excessive use of e-technologies.
- The school has the right to confiscate electronic devices, and to search for and delete information from them, as per the school Behaviour Policy.

## Images

- Pupils must attain the permission of the subjects of all digital images and agree the purpose of their use, before using them.

C:\Users\jday\OneDrive\Documents\Documents\2018-2019\website\School\_E-safety\_policy\_2016\_2017 (1).doc

- Publication of video/still images is subject to the approval of the participants and where appropriate, parents/guardians.
- Images of pupils/use of names may not be published for access externally without the permission of the Headteacher/ Assistant Head, unless covered by the relevant parent consent form.
- When using digital images, staff should inform and educate students/ pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing images on the internet e.g. on social networking sites.

### **Information**

- Pupils may only take digital information from school (via USB or VLE) with the permission of a member of staff. The information should be focused on learning.
- During ICT lessons, pupils will be made aware of plagiarism, quality, accuracy, bias and relevance of information. This work will be followed up when cross-curricular opportunities arise.

### **Communication**

- Students/ pupils should be taught about email safety issues, such as the risks attached to the use of personal details and conversing with strangers. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- The school will actively promote e-safety events for pupils within the school environment ensuring that talks and sessions are age appropriate
- The school will encourage parents and carers to manage and discuss e-safety with pupils at home. This includes active promotion and organisation of e-safety events within the school environment aimed specifically at Parents and carers. These communications are added to the website.
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must only take place on official (monitored) school systems.
- All incidents must be reported by the pupil to the class teacher, who can inform e-safety contact – Mrs Jane Day who will log event and discuss with DO if necessary.

### **Monitoring and Review**

- Incidents must be logged in the E-Safety log book by Mrs Jane Day – these logs are stored in the Foundation Stage Unit filing area.
- Staff will be kept up to date with developments via staff meetings/training.
- Parents and carers will be kept up to date with issues arising with e-safety through school communications such as the 'Friday Flyer' and Parent mail.
- Relevant governors will be kept up to date with developments via meetings and training.