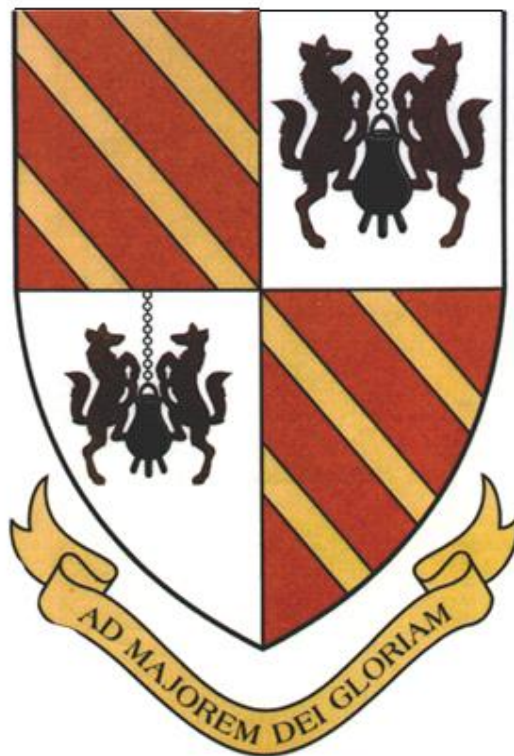


# Loyola Preparatory School Policy for E-Safety

*“Loyola Preparatory School will strive to instil recognition of the talents and achievements of all its members. It will seek to identify and develop a range of skills , techniques and abilities within its pupils which will serve the individual in future life, but will also be put to use as an expression of the Greater Glory of God, both in the personal development of the self and in service to others and the community.”*



*Ad Majorem Dei Gloriam  
To the Greater Glory of God*

# E-Safety Policy

**This policy applies to all pupils at Loyola Preparatory School including those in Early Years Foundation Stage.**

Computing and the use of digital devices is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Computing and ICT covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of computing within our society as a whole. Currently the apps and software children and young people are using both inside and outside of the classroom include:

- Websites
- Podcasting
- Coding
- Gaming
- Mobile devices
- Video & Multimedia

Whilst exciting and beneficial, all users need to be aware of the range of risks associated with the use of these technologies.

At Loyola Prep School we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of fixed and mobile internet technologies provided by the school. Any visitors using their own devices within school, adhere to the schools Acceptable Use Agreement and this e-safety policy.

## **Roles and Responsibilities**

As e-safety is an important aspect of strategic leadership within the school, the Head and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-safety co-ordinators of Loyola Preparatory school are computing coordinator Martena Carrig and Gary Tong for internet filtering.

This policy, supported by the school's acceptable use agreement, is to protect the interests and safety of the whole school community. It is linked to the following school policies: computing, child protection, behaviour, health and safety, anti-bullying and PHSEE.

## **Managing the school e-safety messages**

We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used. These messages will be appropriate to the age of the children being taught.

E-safety guidelines and the SMART rules will be prominently displayed around the school.

As a school, each year, we also participate in e-safety activities during Safer Internet Day.

## **E-safety in the Curriculum**

The school provides opportunities within a range of curriculum areas to teach about e-safety.

Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-safety curriculum.

The teaching of e-safety focuses on helping children to recognise inappropriate content, conduct, contact and commercialism and helps them learn how to respond or react appropriately.

Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues.

Pupils know how to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Childline.

### **Security, Data and Confidentiality**

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.

When accessing, amending and saving any data or information, relating to the school or pupils, school staff follow the guidelines set out in the General Data Protection Regulations 2018.

### **Managing the Internet**

All internet activity within school is a monitored and filtered system. Whenever any inappropriate use is detected, the ICT Manager is notified and the incident will be followed up in line with the school Acceptable Use Policy.

The school maintains students will have supervised access to Internet resources (where reasonable) through the school's digital devices.

If Internet research is set for homework, staff will remind students of their e-safety training. Parents are encouraged to support and supervise any further research.

### **Infrastructure**

The administrative devices throughout school and curriculum access are managed by the school's ICT Manager.

Staff and students are aware that should they encounter or access anything unsuitable or damaging they must report it immediately to the computing co-ordinator or the ICT Manager.

### **Mobile Technologies**

#### **Personal Mobile devices (including phones)**

The school allows staff to bring in personal mobile phones and devices for their own use during designated times outside of the classroom. These are not to be used at any time whilst children are present.

The school is not responsible for the loss, damage or theft of any personal mobile device.

### **Managing email**

The use of email within school is an essential means of communication for staff.

Although pupils currently have access to individual email accounts within school this is not yet widely used.

Staff must use the school's approved email system for any school business.

Staff must inform the e-safety co-ordinator/ line manager/ ICT Manager if they receive an offensive or inappropriate e-mail.

### **Social Networking**

The school does not permit the pupils to access their private accounts on social or gaming networks at any time during the school day.

The school also strongly discourages children from using age inappropriate social networking outside of school. Should the staff be made aware of incidents or activities on these social networks, which has a

direct effect on the children's behaviour or attitudes within school, then the school reserves the right to take action regarding their accounts. This may include discussions with parents, information letters or reporting the child's access to the respective organisations/companies.

## **Safe Use of Images**

### **Creation of videos and photographs**

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

All staff are aware of specific children (they have responsibility for) in school which do or do not have photograph permissions. If they do have permission, staff are aware of which platforms they can be used on.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes field trips. School's own mobile devices must be used in this case.

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

All parents/guardians will be asked to give permission to use their child's work/photos in publicity materials or on the school website, twitter account or mobile app.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.

Parents/ carers may withdraw or amend permission, in writing, at any time.

Two or more forms of ID will not be published alongside their image and vice versa on the school website, twitter account, mobile app or any other school based publicity materials.

### **Storage of Images**

Images/ films of children are stored securely on the school server and / or teacher's individual school laptops/devices.

### **Complaints**

Complaints or concerns relating to e-safety should be made to the e-safety coordinators, line manager or ICT Manager.

### **Inappropriate material**

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the teacher, e-safety coordinators or ICT Manager.

Deliberate access to inappropriate materials by any user will lead to the incident being logged and then forwarded to the e-safety co-ordinator. Depending on the seriousness of the offence; investigation may be carried out by the Head. Staff are aware that negligent use or deliberate misconduct could lead to disciplinary action.

### **Equal Opportunities**

#### **Pupils with additional needs**

The school endeavours to deliver a consistent message to parents and pupils with regard to the schools' e-safety rules.

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety.

Internet activities are planned and well-managed for these children and young people.

Revised January 2022

Review January 2023