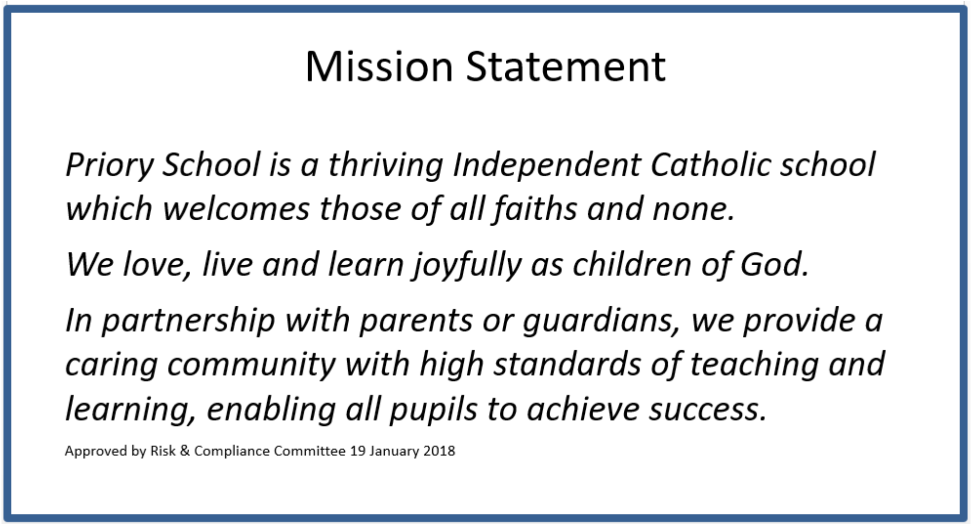
PRIORY SCHOOL
EDGBASTON

ONLINE SAFETY POLICY



Mission Statement

Priory School is a thriving Independent Catholic school which welcomes those of all faiths and none.

We love, live and learn joyfully as children of God.

In partnership with parents or guardians, we provide a caring community with high standards of teaching and learning, enabling all pupils to achieve success.

Approved by Risk & Compliance Committee 19 January 2018

1. The governors and staff of Priory School are committed to providing a fully accessible environment which values and includes all pupils, staff, parents and visitors regardless of their education, physical, sensory, social, spiritual, emotional or cultural needs.

2. The staff, governors and pupils are committed to the safeguarding and welfare of pupils and staff.

3. To meet the needs of our school community all our policies, including this one, can be made available in different formats such as different font sizes or styles, colour or alternative languages.

4. The governing body understands that it has responsibility for ensuring the effective oversight of this policy and will assess, evaluate and review as necessary.

Independent Schools Inspectorate Guidance

Pupils will often have access to technologies that have both positive and negative potential. Consideration should be given to the use of technology within the school setting and beyond, with a policy that is clear, understood and respected by staff, students and the wider school community. Whilst each school's perspective and practice will vary, the policy should ensure the school's expectations and safeguarding obligations are communicated and effective. This Policy includes the Early Years Foundation Stage. A policy should include guidance on:

(a) Clearly defined roles and responsibilities for online safety as part of the school's wider safeguarding strategy and how this links with other safeguarding policy;

(b) Clear guidance on the use of technology in the classroom and beyond for all users, including staff, students/pupils and visitors that references permissions/restrictions and agreed sanctions;

(c) Detail the school's technical provision/infrastructure and the safeguards in place to filter and monitor inappropriate content and alert the school to safeguarding issues;

(d) Detail on how the school builds resilience in its students to protect themselves and their peers through education and information;

(e) Detail on staff safeguarding professional development that includes online safety;

(f) Reporting mechanisms available for all users to report issues and concerns to the school and how they are managed and/or escalated;

(g) How the school informs, communicates with and educates parents/carers in online safety;

(h) The management of personal data in line with statutory requirements.

PRIORY SCHOOL

Rationale

In partnership with parents, Priory School provides a caring community with high standards of teaching and learning. The School embraces the positive impact and educational benefits that can be achieved through the appropriate use of the internet and associated communication technologies, but we are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. Priory School therefore aims to provide a safe and secure environment which not only protects all people on the premises but also educate them on how to stay safe in the outside world.

Publicising Online Safety

Effective communication across all areas of the school community to achieve the school vision for safe and responsible Internet use. To achieve this Priory School will

- Make this policy and the acceptable use policy available on the school
- Introduce this policy at Board level at least once per year or whenever it is updated
- Post relevant Online Safety information in all areas where computers are used.
- Provide Online Safety information to parents.
- Use appropriate resources to enable the teaching of Online Safety to pupils within P.S.H.E.E lessons and Computing –taught in year 7 as a standalone unit in the senior school. In the preparatory school – taught discreetly in ICT lessons and taught as appropriately with in the scheme of work for ICT and P.S.H.E.E.

Scope, Roles and Responsibilities

The Head and Governors have ultimate responsibility for establishing safe practice and managing Online Safety issues at Priory School. The role of Online Safety co-ordinator has been allocated to both the Computing Curriculum co-ordinator and the ICT Manager. They will be the central point of contact for Online Safety and be responsible for day to day issues.

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 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. Curriculum use should be planned, task-orientated and educational. However,*UK Council for Child Internet Safety (UKCCIS) (2018)* in conjunction with *Keeping children safe in Education (2018)* has identified and produced an action plan to help schools to address the dangers of Internet use in the wider non-academic world.

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 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 to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Younger children in the EYFS only access information in school with adult support and guidance. Children are taught to be vigilant when using the internet and social media if used at home. Social media websites are filtered at school. Learn pads are a closed system and only allow content that is specifically chosen by the teacher.

Information system security

Priory School endeavours to provide a safe environment and reviews both physical and network security regularly to monitor who has access to our systems.

Computer networks, including those which may be accessed via the Internet, are an important aspect of information technology education. However, they present possible risks to the spiritual, moral and social development of pupils, particularly in terms of the nature of some of the material, which may be obtained via the Internet. The school uses BLOXX software to filter inappropriate material. This is a system that constantly updates itself and filters inappropriate material for both pupils and teachers alike. In addition teachers can email the Technical team to inform them of anything that slips through (as with the best will in the world, no system is fool proof) and the team can then block those sites if necessary.
As standard:

- Install anti-virus on all computers and update regularly
- Provide central filtering. All staff and pupils understand that if an inappropriate site is discovered it must be reported to the Online Safety co-ordinator who will arrange for the site to be blocked. All incidents will be recorded by the Online Safety co-ordinator using the appropriate Online Safety Incident Forms for audit purposes.
- All staff are issued with their own username and password for network access. Visitors/Temporary staff are dealt with as, and when, a request is received.
- Lock down of desktops that have been inactive for a period of 20minutes.
- Key stage 1 pupils have class logins, supervised by a member of staff.
- Key stage 2, 3 and 4 pupils have their own, individual logins and passwords and understand these cannot be shared.

E-mail

- All teaching staff are given a school e-mail address and understand that this must be used for professional communication.

- All pupils are given a school email address that can be used for educational purposes.

- Everyone in the school understands that the email system is monitored and should not be considered private communication.

- Staff are allowed to access personal email accounts on the school system outside normal class times and understand that any messages sent using school equipment should be in line with the email policy. In addition, they also understand that these messages may be scanned by the monitoring software.

- Everyone in the school understands that any inappropriate emails must be reported immediately to the class teacher/Online Safety co-ordinator.

Published content and the school web site

The Headmaster takes responsibility for content published on the school website but delegate's general editorial responsibility to the Marketing manager.

Publishing pupil's images and work

- Photographs 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 Web site or associated social media, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Social networking and personal publishing

- The school will block 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.

Managing filtering

- The school ensures systems that are in place to safeguard pupils are continually reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Coordinator.

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.

Protecting personal data

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is: used fairly, lawfully and transparently.

Online Safety Training

The School is completing an assessment of current staff skills and will create a program of continuing professional development that includes school inset, in school support and course attendance if required.

Authorising Internet access

All staff must read and sign the Code of Conduct agreement that includes the acceptable use guidelines, 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.

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 ICT provision to establish if the Online Safety policy is adequate and that its implementation is effective, this will be an on-going process undertaken by the Online Safety steering group that is newly in place.

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 Headmaster.

- Complaints of a child protection nature must be dealt with in accordance with the school's child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

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. The pupils will be taught how to remain e-safe, by using CEOP's and other third party resources together during P.S.H.E.E lessons and

ICT lessons. These topics are regular and consistent to ensure that resilience in students is fostered with regard for taking responsibility for their online safety.

Pupils will be informed that network and Internet use will be monitored.

Sanctions

The Behaviour, Anti-Bullying and/or Safeguarding policies may be applied to any misuse of the email or online resources inside or outside of school.

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 will be required to sign and date the acceptable use statement, which outlines the rules surrounding the use of Internet within school.
- Staff will be required to use the CEOP's resources to enable the teaching and learning of Online Safety for the pupils in their care.

Enlisting parents' support

Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school website.

Monitoring and Review

The curriculum and school procedures are constantly being reviewed to take account of educational initiatives and respond to the future priorities of the school.

This policy will be monitored by the Assistant Head teacher, on a regular basis.

Policy reviewed and revised by D.Griffin & K.Webster September 2018