ST MARY'S SCHOOL HAMPSTEAD

Online Safety POLICY

September 2023

Reviewed: September 2023
Next Review Date: September 2024

MISSION STATEMENT

St Mary's School seeks to provide an education firmly founded on Christ and the Catholic Faith.

Spiritual and moral principles are nurtured in a way that is reflected in daily life.

Within a happy and caring environment and based on the recognition of the dignity and worth of each child, high standards are expected. Intellectual development is emphasised and fostered along with the pursuit of academic excellence.

St Mary's values the unique contribution of every child within the school community.

St Mary's aims to encourage an active partnership between home, school, parish and the wider community.

1 Scope

This policy applies to all members of the school community (staff or pupils) who use school IT systems, as a condition of access. Access to school systems is not intended to confer any status of employment on any contractors.

2 Objectives

2.1 To ensure that pupils are appropriately supervised during school activities.

2.2 To promote responsible behaviour with regard to e-based activities.

2.3 To take account of legislative guidance.

3 Guidance

3.1 The Headmistress will be responsible for the implementation of this policy. This includes taking overall responsibility for ensuring the standards related to monitoring and filtering are being met. This includes ensuring that:

- filtering and monitoring systems are in place
- decisions regarding what is blocked or allowed and the reason for this are documented;
- reviewing the effectiveness of the provision;
- overseeing reports;
- all staff understand their roles, are appropriately training, follow policies, processes and procedures and act on reports and concerns.

This policy should be read in conjunction with the filtering and monitoring checklist (360 Safe).

3.2 The STEAM Leader of Learning will act as E-Safety Co-ordinator, alongside the Designated Safeguarding Lead, and will:

- compile logs of e-safety incidents;

- report to the Headmistress on recorded incidents;
- ensure that staff are aware of this guidance;
- provide / arrange for staff training;
- liaise with school technical staff;
- liaise with the Headmistress on any investigation and action in relation to e-incidents;
- advise on e-safety policy review and development; and
- oversee and act on filtering and monitoring reports; safeguarding concerns; and checks to filtering and monitoring systems.

3.3 The Network Manager will have technical responsibility for:

- implementing and maintaining filtering and monitoring systems;
- providing filtering and monitoring reports;
- completing actions following concerns or checks to the system;
- the IT infrastructure and that it is not open to misuse or malicious attack;
- ensuring that users may only access the networks and devices through an enforced password protection policy; and
- ensuring that the use of the network (including internet, virtual learning, email and remote access) is monitored for misuse and is maintained.

The Network Manager will keep up to date with e-safety technical information in order to carry out their role.

3.4 Teaching and Support Staff will:

- maintain awareness of school e-safety policies and practices;
- ensure they have read, understood and signed the staff IT Acceptable Use Policy;
- report any suspected misuse or problem to the Headmistress or E-Safety Co-ordinator;
- ensure that all digital communications with pupils / parents / carers/ fellow staff are on a professional level and conducted on school systems;
- where relevant e-safety is recognised in teaching activities and curriculum delivery;
- ensure pupils understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;
- monitor the use of digital technologies (including mobile devices, cameras etc.) during school activities; and
- ensure that where the use of the internet is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

3.5 Child Protection

Those responsible for child protection (Designated Safeguarding Lead and deputies) should be trained in e-safety issues and aware of the implications that may arise from:

- sharing of personal data;
- access to illegal / inappropriate materials;
- inappropriate contact on-line with adults / strangers;
- potential or actual incidents of grooming; and
- cyber-bullying.

The Designated Safeguarding Lead has lead responsibility for safeguarding and online safety, including overseeing and acting on filtering and monitoring reports, safeguarding concerns and checks on the filtering and monitoring system.

3.6 Pupils

- are responsible for using school digital technology systems, both in school and at home, in accordance with the School acceptable use policy;
- will understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;
- will understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- are expected to understand policies on the use of mobile devices and digital cameras, the taking / using of images and cyber-bullying; and
- will understand that the e-safety policy will include actions outside of School where related to school activities.

3.7 Parents / Carers

- will be advised of e-safety policies through parents' evenings, newsletters, letters, school website, etc.;
- will be encouraged to support the School in the promotion of good e-safety practice; and
- should follow school guidelines on:
  - digital and video images taken at school events;
  - access to parents' sections of the school website / pupil records;
  - their children's / pupils' personal devices in the School (where this is permitted); and
  - their children's conduct and use of technology during any learning carried out via technology in their own home.

3.8 Governors

The Governor with responsibility for Safeguarding will also have strategic responsibility for online safety, including filtering and monitoring, and will need assurance that the standards are being met (this can be offered via the filtering and monitoring checklist and reports presented at Education and Staffing Committee Meetings).

Legal Requirements & Education Standards

References:

A: Handbook for the Inspection of Schools - The Regulatory Requirements, Part 3 (www.isi.net)

B: Reference Gide to the key standards in each type of social care service inspected by Ofsted (www.ofsted.gov.uk)

C: "Health and Safety at Work" Section H of the ISBA Model Staff Handbook,

D: "Health and Safety and Welfare at Work" Chapter N of the ISBA Bursar's Guide

E: "Insurance" Chapter K of the Bursar's Guide by HSBC Insurance Brokers Ltd

F: UK Council for Child Internet Safety (www.edcuation.gov.uk/ukccis)

G: Cyber-bullying.org (www.cyberbullying.org)

H: Department for Education "Safer Working Practice for Adults who Work with Children and Young People" (www.education.gov.uk)