ST. AMBROSE PREPARATORY SCHOOL

POLICY

ON

E-SAFETY

SPRING 2017

Review: Spring 2019

This policy has been written in consultation with staff and governors of St. Ambrose Preparatory School and with due regard to the school's mission statement:

"At St. Ambrose Preparatory School, we strive together to do our very best and to make this a safe, happy place, with Christ the centre of all we do."

St. Ambrose Preparatory School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

St. Ambrose Preparatory School is a Catholic School, which was founded by the Christian Brothers and is a place where the staff and governors work to bring the Gospel values into all areas of School life and where prayer, worship and liturgy are seen as meaningful experiences.

St. Ambrose Preparatory School upholds fundamental British values and encourages respect for all people.

St. Ambrose Preparatory School recognises its legal duty to work with the Local Safeguarding Children's Board acting on behalf of children in need or enquiring into allegations of abuse.

We recognise that pupils have a fundamental right to be protected from harm and require a secure environment in order to learn effectively.

St. Ambrose Preparatory School's Safeguarding Children Policy follows the guidelines laid down by Trafford Council's Safeguarding Children's Procedures and "Working Together to Safeguard Children"(2015) and " Keeping Children Safe in Education"(2016) (KCSIE) and Prevent Duty Guidance (March 2015).

E- Safety Policy (staff are notified of regular ISI updates)

(Incl EYFS, KS1 & KS2)

The Governing Body of St. Ambrose Prep School understands its regulatory responsibilities and will maintain an effective oversight of this policy, by evaluating its effectiveness, and reviewing and implementing change.

Introduction and Philosophy

Computing and ICT in the 21st Century is seen as an essential resource to support teaching and learning, as well as being an important part of everyday life. Consequently, St Ambrose Preparatory School needs to use these technologies in order to arm pupils with the skills to access life-long learning and employment.

This policy is a statement of the aims, principles and strategies for the safe use of the Internet and related technologies at St. Ambrose Preparatory School. This Policy document is drawn up to protect all parties – the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

It has been developed as a result of a process of consultation. It has been agreed by senior managers and approved by Governors.

Aims

The philosophy of 'empowering children to stay safe' includes aims that children are:

- safe from maltreatment, neglect, violence and sexual exploitation;
- safe from accidental injury and death;
- safe from cyberbullying and discrimination;
- safe from crime and anti-social behaviour in and out of school;
- secure, stable and cared for.

Many of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use Computing/ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that Computing/ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;

- An e-Safety education programme for pupils, staff and parents**.**

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The Headmaster ensures that the e-Safety Policy is implemented and compliance with the Policy is monitored.

The responsibility for e-Safety has been designated to Mr. F. Driscoll, Headmaster

Our school **e-Safety Co-ordinator** is, Mr. F. Driscoll, Headmaster

Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance through organisations such as The Child Exploitation and Online Protection (CEOP)[1]. The school's e-Safety coordinator also ensures, senior management and Governors are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any cyberbullying, abuse or inappropriate materials

The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- Websites
- Learning platforms and VLE
- Email, messaging, chat rooms, social networking.
- Blogs
- Podcasting
- Music downloading
- Gaming
- Video broadcasting
- Use of smart phones and other mobile devices that have web functionality.

[1] http://www.ceop.gov.uk/

Accessing the Internet

The school will maintain a current record of all staff who are granted access to the school's electronic communications.

All staff must read and sign the Staff Code of Conduct for Acceptable Internet Use before using the school Computing/ICT resources.

For younger children, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on –line materials.

Parents will be asked to sign and return a consent form for pupil access.

Parents will be informed that pupils will be provided with supervised Internet access.

The Internet and Learning

Effective practice in Internet use for teaching and learning is essential as the quantity of information can be over whelming.

Younger children should be offered selected sites rather than the open Internet search. Older children benefit from the same use of suggested sites and must also be encouraged to evaluate everything they read and to refine their own publishing. Plagiarism is not acceptable at any times. Children will be taught to acknowledge sources in their work.

The school internet access will be designed expressly for pupil use and will include filtering appropriate to primary school children.

Pupils will be taught what Internet use is acceptable and what is not, and given clear objectives for Internet use.

At present, these rules are based on Childnet's SMART rules for children:-

S – Stay **safe**, do not give out personal information
M – Tell an adult if you are thinking of **meeting** someone.
A – **Accepting** e-mails or open attachments from people you do not know can lead to viruses and unwanted emails.
R – Information you find on the Internet may not be **reliable** and people may not be who they say they are.
T– **Tell** a parent, carer or trusted adult if someone or something makes you feel uncomfortable or worried, and if you or someone you know is being bullied online.

Other teaching tools include the use of e-safety websites including:

Think U Know	(www.thinkuknow.co.uk)
Kidsmart	(www.kidsmart.org.uk)
Espresso	(www.espresso.co.uk)

E-mail

E-mail is an essential means of communication for staff, however it is only to be used for Professional dialogue or discussion. At present it is the school policy that no pupils have school e-mail accounts

Website

Contact details on the website will include school address, e-mail and telephone number. Staff or pupils' personal details must not be published.

No link should be made between an individual and any home address (including simply street names);

The Headmaster will take overall editorial responsibility to ensure that content is accurate and appropriate.

The school must respect intellectual property rights and copyright.

The publishing of pupils' names with their images is not acceptable. Images should be carefully chosen so that individuals can not be identified.

Written permission will be sought from parents before publication of any images on the web site or newsletter.

Work can only be published with the permission of pupil and parents.

Social Networking

Examples of social networking sites include- blogs, MySpace, MSN space, bulletin boards, chat rooms, instant messaging and many others. As children can access these at home, advice to children will be supplemented by similar advice to their parents.

School will block access to these sites and others.
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 and / or their location. Pupils will be advised not to place personal photos on any social network space. This is reinforced during e-Safety lessons.

Staff are also encouraged to review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.

Although these networks are used by staff in their own time, staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks.

It is never acceptable to accept a friendship request from a child from the school as in almost all cases children of primary age using such networks will be breaching the terms and conditions of use of those networks. It is also extremely inadvisable to accept as friends ex-pupils who are still minors.

Managing Filtering

At present, St. Ambrose Preparatory School uses 'Censor net', a dynamic service which filters Internet sites and we also endeavour to block unsuitable sites as reported.

To this end we will:-

Work with our Internet Service Provider and our Technical Support to ensure that systems to protect pupils are reviewed and improved.

Technical Support will ensure that the virus protection is up to date at all times.

If staff or pupils discover unsuitable sites, the URL must be reported immediately to the Computer Specialist teacher/ and or ICT Co-ordinator and the e-Safety Coordinator.

Any material that the school believes is illegal must be reported to appropriate agencies such as CEOP.

It is the responsibility of the members of staff to ensure their computers, emails etc are password protected and should any issues arrive they must report to the Technical support.

Mobile Phones and other electronic devices

Mobile phones and other electronic devices should not be used in school time. For safety and security all pupils at the start of the school day are required to surrender their mobile phones/electronic devices into the school office. These will be kept in a locked box and boys can collect on leaving the school at the end of the day. Staff may keep phones with them during the school day but it is not acceptable to have them on view in the classroom and responding to calls/messaging there is forbidden. The sending of abusive or inappropriate text messages is strictly forbidden and will result in disciplinary action. ***For staff use see Code of Conduct for ICT and for pupils see Health, Safety & Welfare Policy***

Use of Portable Equipment

The school provides ICT equipment such as laptop computers (for staff) and digital cameras to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities.

Exactly the same principles of acceptable use apply as in other sections of this policy:

- Certain items (laptops) will remain in the care of Technical Support, who will keep a record of all portable equipment that has been allocated to staff.

- Equipment such as laptop computers can be taken offsite for use by staff in accordance with the E-Safety Policy and the equipment is fully insured from the moment it leaves the school premises. The cover excludes theft or attempted theft from an unattended vehicle unless the vehicle is locked, there are signs of forced entry and the property is out of sight in a locked compartment or boot within the vehicle.

- Any costs generated by the user at home, such as phone bills, printer cartridge etc. are the responsibility of the user;

- Where a member of staff is likely to be away from school through illness, professional development (such as secondment etc.) or maternity leave, arrangements must be made for any portable equipment in their care to be returned to school. In the event of illness, it is up to the school to collect the equipment if the individual is unable to return it;

- If an individual leaves the employment of the school, any equipment must be returned;

- The use of USB pens etc. must be regulated. Where information has been downloaded from the internet, or copied from another computer, wherever possible, it must be emailed to school to ensure that it undergoes anti-virus scanning. If this proves to be impossible, (due to file size, technical difficulty etc.) express permission must be sought from the ICT coordinator and the support team prior to the data being transferred;

- No other software, whether licensed or not, may be installed on laptops in the care of teachers as the school does not own or control the licences for such software.

Managing emerging technologies

- Emerging technologies will be examined for educational and risk assessment will be carried out before it is allowed to be used in school.

- Any mobile phones brought into school by pupils will be taken to the school office and kept there till the end of the day.

- In the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner.

Roles and Responsibilities

Responding to an incident of concern

Our e-Safety Coordinator acts as first point of contact for any complaint.

Complaints of Internet misuse will be dealt with by a senior member of staff

In the event of children being unintentionally exposed to undesirable materials the following steps will be taken:

1. Pupils should notify a teacher immediately.
2. The e-Safety Coordinator should be notified and the incident reported.
3. The incident should be recorded in a central log by which the school may reliably report the frequency and nature of incidents to any appropriate party.

4. The child's parents and/or the School Governors should be notified at the discretion of the Head according to the degree of seriousness of the incident.

Children must never intentionally seek offensive material on the Internet. Any transgression should be reported and recorded as outlined above. Any incident will be treated as a disciplinary matter and the parents of the child or children will normally be informed. If deliberate access to undesirable materials is found to be repeated, flagrant or habitual the matter will be treated as a serious disciplinary issue. The child or children's parents will be informed and the Governing body advised.

Staff and pupils are given information about infringements in use and possible sanctions.

Sanctions available include:

- interview/counselling Headmaster/e-Safety Coordinator;
- informing parents or carers;
- removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system;
- Referral to relevant authorities
- Permanent or Temporary exclusion.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school child protection procedures.

Staff

All staff will be given the School e-Safety Policy and its application and importance explained.

Staff are required to read and sign a ‘Code of Conduct’ regarding Acceptable Use of the school’s information system. (See Appendix 1)

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

The ICT Technician (Technical Support), who at present manages the filtering systems, will be supervised by senior management and has clear procedures for reporting issues.

Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

Any complaint about staff misuse must be referred to the Headmaster.

Parents

Parents' attention will be drawn to the school's e-Safety Policy in newsletters, and on the school website.

When joining the school, parents are required to read and agree to the school's Statement of Acceptable Use for ICT.

A partnership approach with parents such as meetings and or regular mailing will be encouraged.

Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents. Relevant websites include:
CEOPs, Childline, childnet and parentzone.

Specific Learning Needs

Provision for children with specific learning needs in relation to e-Safety is made after discussion between class /subject teacher, support staff and the SENCO.

Some groups of children are potentially more vulnerable and more at risk than others when using ICT/Computing. These can include children with emotional or behavioural difficulties, learning difficulties, and other complex needs, as well as those whose English is an additional language, and looked after children.

Children with Specific Learning Needs can use the internet in educational, creative, empowering and fun ways, just like their peers. However, they may be particularly vulnerable to e-safety risks. For example:

- Children and young people with Autism Spectrum Disorder may make literal interpretations of content, which will affect how they respond;
- Some children may not understand much of the terminology due to language delays or disorders;
- Some children with complex needs do not understand the concept of friendship, and therefore trust everyone implicitly. They do not know how to make judgments about what is safe information to share. This leads to confusion about why you should not trust others on the internet;
- There is also growing concern around cyberbullying. We need to remember that some children with Specific Learning Needs or disabilities may be vulnerable to being bullied through the internet, or not recognise that they are being bullied;
- In addition, some children may not appreciate how their own online behaviour may be seen by someone else as bullying.

Where appropriate, special adaptations, such as video presentations with signing and the use of Widgit cards for poorer readers, of Childnet International's SMART resources can be accessed.

Teachers should tackle these sensitive issues sympathetically.

The SENCO should ensure that strategies for safe internet use are part of individual children's learning plan.

Equal Opportunities

All teaching and non-teaching staff at St. Ambrose Preparatory School are responsible for ensuring that all children, irrespective of gender, ability, ethnicity and social circumstances, have access to the whole curriculum and make the greatest possible progress. Equal access needs to be planned and monitored very carefully and this must be reflected in teacher's pairs and groupings. General monitoring is the responsibility of the Headmaster, and senior management.

Where use of a school computer proves difficult for a child because of a disability, the school will provide specialist equipment and software, so that the pupil may have access. (i.e. lower case lettering on keyboards, concept keyboards, roller ball mouse, filter screens.) Pupils with learning difficulties can also be given greater access to the issues of e-Safety through the use of Computing/I.C.T.

Review

The speed and nature of development is such that a review of the e-Safety Policy should take place on a bi-annual basis. The ICT Co-ordinator then makes any changes or adaptations of policy. Throughout the year, all staff are encouraged to feedback information about the effectiveness of this policy and ideas to the co-ordinator.

Appendix 1

ST. AMBROSE PREPARATORY SCHOOL

Staff Code of Conduct for ICT

To ensure that you as members of staff are fully aware of your professional responsibilities when using information systems and when communicating with pupils, you are asked to sign this code of conduct. Members of staff should also consult the school's e-safety policy for further information and clarification.

The computer system is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The Internet facility will be available during term time only. The school reserves the right to examine or delete files where it believes unauthorised use of the information system may be taking place, or to monitor any Internet sites visited.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner;
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDA's, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business;
- I will not access the system without the use of an authorised account and password, which should not be made available to anyone other than an authorised system manager;
- I understand that school information systems may not be used for private purposes without specific permission from the Headmaster;
- I will not install any software or hardware without permission;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- I will respect copyright and intellectual property rights;
- I will ensure that electronic communications with pupils including email, and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted;
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing;
- No e-mail attachments must be opened unless you are absolutely sure they are from known associates. If you are unsure, always delete it straight away without opening it as this is the major route for computer viruses;
- Posting anonymous messages and the forwarding of chain letters is forbidden, as is the use of public chat lines;
- I will keep my personal mobile phone in my bag/stockroom during the school day and only use in my own time at break/lunchtime and I am aware it cannot be used when children are present; If required I can take my personal mobile on a school trip but must not use it to take photographs;
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance;
- I will report any incident of concern regarding children's safety to the e-Safety Coordinator, the Designated Children Protection Coordinator or Headmaster;
- I understand that access to undesirable materials by adults is unacceptable and will be treated as a disciplinary issue. If abuse is found to be repeated, flagrant or habitual the matter will be treated as a very serious disciplinary issue and the Governors will be advised.

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed : ……………………………. Capitals: …………………… Date: ……………………..

Accepted for School: …………………………………… Capitals: …………………………

Appendix 2

Dear Parents,

Internet Access for Pupils

At St Ambrose, as a part of our ICT programme, we offer pupils supervised access to the Internet. As part of our ‘Acceptable Use of ICT’ policy, we are seeking your permission for your child to use the Internet in school.

Internet access has many educational benefits by enabling children to explore many libraries and databases. Although Internet use is supervised, we must be aware that some pupils may access information that is inappropriate or potentially offensive to some people. We believe that the benefits of Internet access far outweigh the disadvantages.

During school, teachers will guide pupils towards appropriate material. At home, families bear the same responsibility for guidance as they exercise with other information sources such as television, telephone, films and radio.

Please read the ‘Acceptable Use of ICT Policy’ and then complete the enclosed form and return it to school as soon as possible.

Yours sincerely,

Mrs Louise Fielding

ICT Co-ordinator

Appendix 2

ST AMBROSE PREPARATORY SCHOOL

Acceptable Use of ICT

1. Software available to the children on the network has been designed specifically for their use and as such, its content is appropriate. Use of additional software, CD-ROMs etc should be monitored by the ICT co-ordinator and the class teacher before use by the children.

2. Internet access is made available by an approved ISP for schools and is filtered for undesirable materials. In addition, staff are advised to be vigilant and explore any proposed sites before allowing the class access. Use of search engines is to be strictly controlled under the supervision of the class teacher only.

3. Staff in charge of Internet based research projects need to be aware of their content. They are also required to highlight the importance of respecting copyright and avoiding plagiarism to any child involved in such a project.

4. Computers are sited such that what is on the screen can be easily seen.

5. Before our children use the Internet in school, we require that their parents are made aware of the school's Policy for Acceptable Use and sign the 'Internet Permission Form'.

6. When children are first introduced to the Internet at school, they are given guidance on sensible and responsible use, in line with 'Our Internet Rules'. They are required to sign a pledge that, when they access the Internet at school, it will be in accordance with our rules. In particular they are instructed that they are required to report any upsetting materials to a member of staff straight away.

Appendix 2

ST AMBROSE PREPARATORY SCHOOL

These rules will help us to stay safe when using ICT at school

1. I cannot use school ICT equipment until my parent/s and I have signed my use agreement form and the completed form has been returned to school.
2. I can only use the computers and other ICT equipment for my schoolwork and only with my teacher's permission.
3. I can only go online or use the Internet at school when a teacher gives permission and an adult is present.
4. If there is anything I'm not sure about I will ask my teacher.
5. I will not use the Internet, email, mobile phones or any other ICT equipment to be mean, rude, or unkind to or about other people.
6. If I find anything that upsets me, is mean or rude, or things I know are not acceptable at our school, I will not show others; I will turn off the screen and get a teacher straight away.
7. I must not bring any ICT equipment/devices to school. This includes things like mobile phones, iPods, games, cameras, USB drives and software.
8. I will ask my teacher's permission before I put any personal information online. Personal information includes:
   - Name
   - Address
   - Email address
   - Phone number
   - Photos
9. I will be careful and will look after all our school ICT equipment by:
   - Not being silly and playing around
   - Following our school ICT rules
   - Telling a teacher about anything wrong or damaged
10. I understand that if I break these rules the school may need to tell my parent/s.

Please detach and return this section to school.

✂____

<u>ICT Rules</u>

I have read the 'Acceptable use of ICT' agreement and I am aware of the school's initiatives to maintain a safe ICT learning environment, including my child's responsibilities.

Name of pupil: ___________________________________ **Year:** ___________

Parent's signature: _________________________________

Pupil's signature: __________________________________

Date: ________________________