LORETO PREPARATORY SCHOOL

Dunham Road, Altrincham, Cheshire WA14 4GZ

Telephone: 0161 928 8310

Registered Charity No. 25060

E-SAFETY POLICY

Mission Statement

At Loreto Preparatory School
We are eager and inspired to do our best,
Meeting the challenges and opportunities of a changing world
With love in our hearts.

We are called to be joyful and prayerful,
Living the Gospel and the Catholic faith
And celebrating the values of Mary Ward
With our parents and the whole Loreto family.
Women in time to come will do much.
Mary Ward

This policy has been written with regard to and in the spirit of our school aims, in particular to enable children:
'To feel secure and valued within a safe and well-maintained environment.'
'To be happy and confident and have a good sense of humour.'
'To have a good understanding of the world and to be adaptable to change.'
'To be honest citizens and make a contribution to society.'

This policy applies to all members of the school community, including staff, pupils, volunteers, parents, carers and visitors who have access to and are users of school ICT systems, both in and out of the school. It includes the Early Years Foundation Stage and before and after school provision and activities. It takes account of the current Keeping Children Safe in Education (KCSIE), current Independent School Standards Regulations and Working Together to Safeguard Children (2015).

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of inappropriate e-safety behaviour, including attempts to bully, groom, abuse or radicalise children out of school. The use of technology is now a significant factor in many safeguarding issues. The school approach is to educate its community in the use of technology and protect them from its mis-use by establishing mechanisms to identify, intervene in and escalate any incident where appropriate.

The three main areas of risk are:

- Content, ie being exposed to illegal, inappropriate or harmful material.
- Contact, ie being subjected to harmful online interaction with other users.
- Conduct, ie personal online behaviour that increases the likelihood of, or causes of harm.

The school is aware that 'over-blocking' should be avoided in order not to restrict what children should be taught with regards to technology. Governors and staff realise and support this.

Roles and Responsibilities

The nominated governor responsible for Child Protection, which includes e-safety is Mrs Nora Griffin. Her role includes:

- regular meetings with the e-safety co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to the Board of Governors

The Head Teacher

The Head Teacher is the e-safety co-ordinator and the Designated Safeguarding Lead (DSL) for Child Protection in the school.

The e-safety co-ordinator / DSL

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy.
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- ensures that the Fundamental British Values are promulgated throughout the curriculum.
- makes staff aware of the mechanisms and ramifications of initiatives such as Prevent.
- provides training and advice for staff, including online safety, Prevent and Channel information..
- liaises with the Trafford Local Authority Designated Officer where appropriate, or the police in the event that there is a concern about radicalisation.
- liaises with school technical staff.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- meets regularly with the e-safety governor to discuss current issues and review incident logs.
- reports regularly to the Senior Leadership Team.

ICT Service Provider

It is the responsibility of the school to ensure that the ICT service provider carries out all the e-safety measures below. The ICT service provider is fully aware of the school e-safety policy and will ensure:

- that the school's technical infrastructure is secured by virus protection and is not open to misuse or malicious attack
- that filtering/monitoring software / systems are implemented and updated as agreed with the e-safety co-ordinator and the ICT co-ordinator. Systems must be sufficiently rigorous as to ensure that children are safe from terrorist and extremist material, whilst ensuring this does not impede the teaching of online safety.
- that children's access to school computers is password protected.

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters including the dangers of grooming and radicalisation. They should have a sound knowledge of the current school e-safety policy and practices.
- as part of the PSHEE and Computing curricula, the children are helped to understand the risks posed by adults or young people who use the internet and social media to bully, groom,
- abuse or radicalise children. This training will also take place on a very regular basis, where IT is used to deliver or support the curriculum.
- they report any suspected misuse or problem to the head teacher for investigation.
- all digital communications with students / pupils / parents are on a professional level and only carried out using official school systems.
- e-safety issues are embedded in all aspects of the curriculum and other activities.
- pupils understand and follow the e-safety procedures provided by the school.
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities and implement current policies with regard to these devices.
- when using digital images, they inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images.
- in lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use.
- in their personal use of social media, no reference whatsoever is made to the school community.
- their security settings are reviewed regularly.

Pupils

- Pupils are required to sign an internet use agreement (see appendices 2 and 3below).
- will be given information on and reminders about e-safety on a very regular basis in all aspects of the curriculum, particularly in computing and PSHE, and will be taught how to protect themselves and their peers.
- will be taught the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand policies on the use of mobile devices and digital cameras, and on the taking / use of images and on cyber-bullying.
- will be taught the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-safety Policy covers their actions out of school, if related to their membership of the school.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully.
- Written parental permission will be sought before children's photographs are published.

Social networking and personal publishing

The school will deny access to social networking sites and students will be advised not to use these at home.

Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line pupil records
- their children's personal devices in the school (where this is allowed)

Data Protection

In accordance with the Data Protection Act 1998, the school will ensure that:

- it will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- at all times, staff will take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse. Electronic devices containing personal details are password protected.
- parents may only access their own child's records stored on the EYFS tracking system (Tapestry). They are required to set up password protected access for this purpose.
- parents are asked to sign that they agree to their child's biometric identification details being used for the library system.

Monitoring and Review

This policy will be reviewed regularly by the Head Teacher and SLT. Advice and information from the ICT Provider and the staff involved will be taken into account. This policy will be reviewed annually by Governors and any weaknesses or deficiencies will be rectified without delay.

Useful Internet Sites for information and support:

The UK Safer Internet Centre (www.saferinternet.org.uk)
CEOP's Thinkuknow website (www.thinkuknow.co.uk)

Last review Spring 2017
Next review Spring 2019

Related Policies

Anti-Bullying
Behaviour Policy
Child Protection/ Safeguarding Policy
Computing Policy
Cyber Bullying Policy
Mobile Devices Policy
PSHEE Policy

APPENDIX 1

Further information about Online Safety

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material;
- contact: being subjected to harmful online interaction with other users; and
- conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Filters and monitoring

Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place. Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn, governing bodies and proprietors should consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks.

The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part by the risk assessment required by the Prevent Duty.

The UK Safer Internet Centre has published guidance as to what "appropriate" might look like:

- UK Safer Internet Centre: appropriate filtering and monitoring

Guidance on e-security is available from the National Education Network-NEN. Buying advice for schools is available here: buying for schools.

Whilst filtering and monitoring are an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a whole school approach to online safety. This will include a clear policy on the use of mobile technology in the school. Many children have unlimited and unrestricted access to the internet via 3G and 4G in particular and the school and college should carefully consider how this is managed on their premises.

Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

Staff training

Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 64) and the requirement to ensure children are taught about safeguarding, including online (paragraph 68), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

Information and support

There is a wealth of information available to support schools and colleges to keep children safe online. The following is not exhaustive but should provide a useful starting point:

www.thinkuknow.co.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.childnet.com/cyberbullying-guidance

www.pshe-association.org.uk

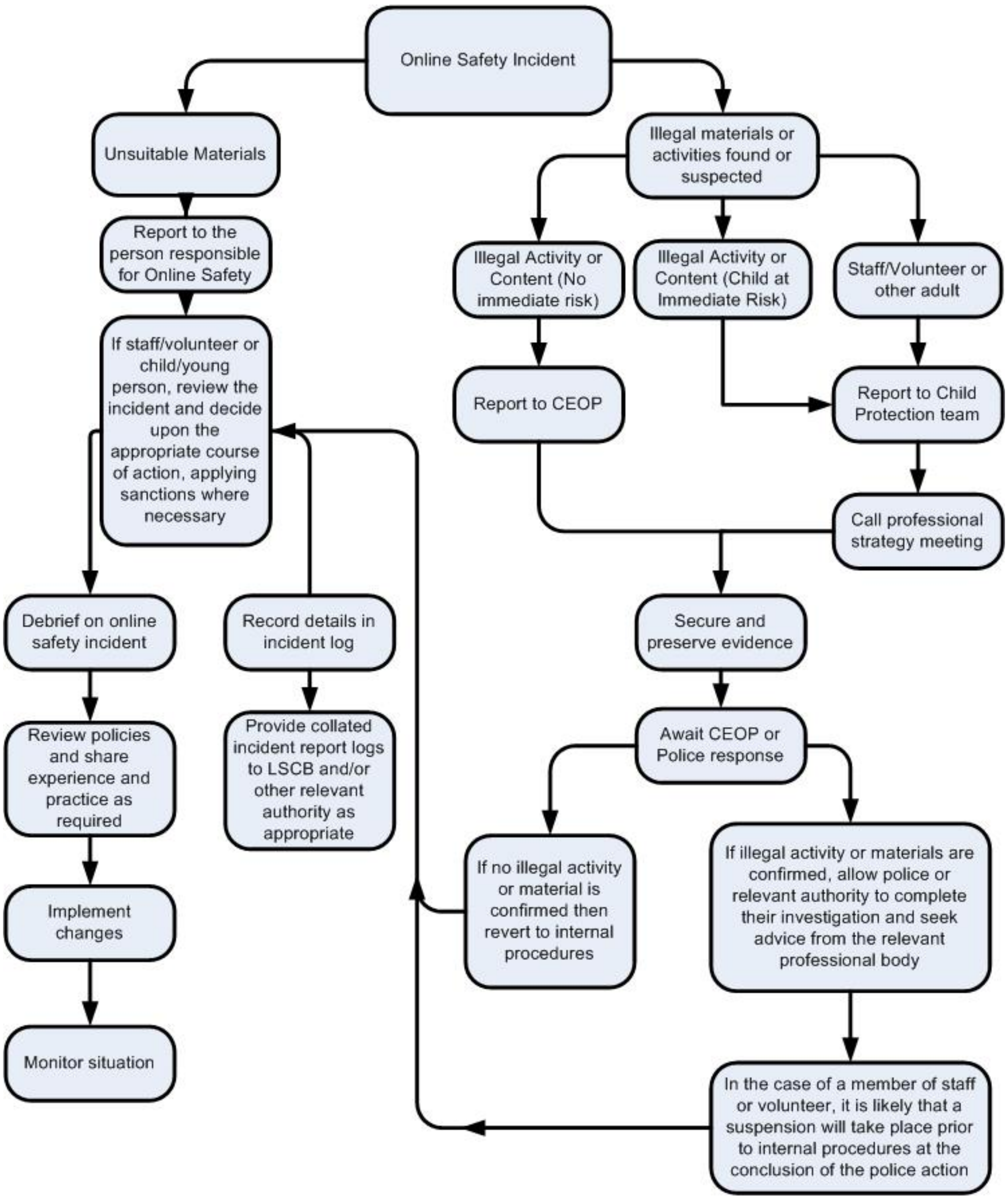
educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

APPENDIX 2

Dealing with Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school / academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in the following procedure should be followed:

- have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- it is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action
- **If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include:**
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

APPENDIX 3

KEY STAGE 2

INTERNET USE AGREEMENT

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult. I have read and understand these rules and agree to them.

Name of Pupil ____

Signature (Pupil)____

Signature (Parent))____

Date______________________________

APPENDIX 4

KEY STAGE 1 and EYFS

INTERNET USE AGREEMENT

This is how I will stay safe when I use the school computers:

- I will ask a teacher or suitable adult if I want to use the computers.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

Name of pupil____

Signed (pupil)____

Signed (parent)____

Date______________________________