Our Lady Queen of Peace

Catholic Engineering College

Whole School Policy for On-Line Safety

Mission Statement

In Christ We Grow – As a learning community we live out our Mission Statement striving for excellence through caring, sharing and achieving.

OUR LADY QUEEN OF PEACE CATHOLIC ENGINEERING COLLEGE

The purpose of this On-Line /E-safety policy is to ensure every child and adult at our school is safe and protected from harm on line, on social media or via mobile technologies.

Education - Students

The education of students in online safety is an essential part of Our Lady's e-Safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety is a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of the ICT /Computing/PHSE lessons and are to be regularly revisited. New guidelines (2019) on 'Sexting' to be included in curriculum IT.
- Key online safety messages are reinforced as part of a planned programme of assemblies and form time / pastoral activities
- Students are expected to be taught in all lessons, to be critically aware of the materials / content they access on-line and be guided to check the accuracy of information.
- Students are expected be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students are helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff act as good role models in their use of digital technologies the internet and mobile devices

- In lessons where internet use is pre-planned, it is best practice that students be 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.
- Where students are allowed to search the internet freely, staff should be vigilant in monitoring the content of the websites the young people visit using Empero monitoring software where available.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- When e-Safety incidents occur students and their parents are made aware of dangers, responsibilities, expectations, etiquette, impact and age related appropriateness of online activities. This is recorded for monitoring purposes in an e-Safety log kept by the e-Safety Co-ordinator.

Education - Parents

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Our Lady's will seek to provide information and awareness of online safety risks and the potential for their children to come across harmful or inappropriate material on the internet or social media. This will be communicated to parents and carers, with guidance on how to respond, through:

- Curriculum activities
- Web site, letters, newsletters
- Parents' evenings
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications *e.g. www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers on the school website*
- *When their children have been involved in on line safety incidents.*

On-Line Safety Training

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school / academy Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- This On-Line Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Coordinator / Officer will provide advice / guidance / training to individuals as required. Change to All Staff annually and as required

Technical – Infrastructure and equipment, filtering and monitoring (below all checked by RED and RC)

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School's technical systems are managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling is securely located and physical access restricted
- All users have clearly defined access rights to school technical systems and devices. This is described in the school Operational Handbook
- All users are provided with a username and secure password by IT Support who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every 42 days.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a password encrypted document on a secure network
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet

Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.

- Internet filtering ensures that children are safe from terrorist and extremist material when accessing the internet.
- The school provides enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc)
- School technical staff regularly monitor and record the activity of users on the school technical systems. Sophos XG firewall logs and Impero classroom management logs are used for this purpose.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
- Appropriate security measures are in place (Sophos AV, Encryption and InterceptX) to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Provision is in place for temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- Guidance regarding the extent of personal use that users staff / students are allowed on school devices that may be used out of school is included in the Operational Handbook
- An agreed protocol is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data should cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. This is communicated through the school Operational Handbook.

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The use of mobile technologies should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Anti - Bullying procedures, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile

technologies should be an integral part of the school's Online Safety education programme.

Use of Digital and Video Images

Staff, parents /carers and students are aware of the risks associated with publishing digital images on the internet or social media. Such images may provide opportunities for cyberbullying to take place. Staff, parents/carers and students should know that digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press
- In order to protect the privacy and danger of images being misused, parents/ carers must not take videos or digital images of their or other children at school events.
- Staff and volunteers are allowed to take video / video images to support educational aims, and must only appear on school platforms, publications and media. They must not be shared on other platforms, publications (except press where permission is given)
- Images should only be taken on school / academy equipment, the personal equipment of staff should not be used for such purposes.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on platforms, publications and media, particularly in association with photographs.
- Student's work can only be published with the permission of the student and parents/carers.

Social Media – Protecting Professional Identity

Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Ofsted's online safety inspection framework reviews how a school protects and educates staff and students in their use of technology, including the measures that would be expected to be in place to intervene and support should a particular issue arise.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided, including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities and procedures
- Risk assessment, including legal risk

School staff should ensure that:

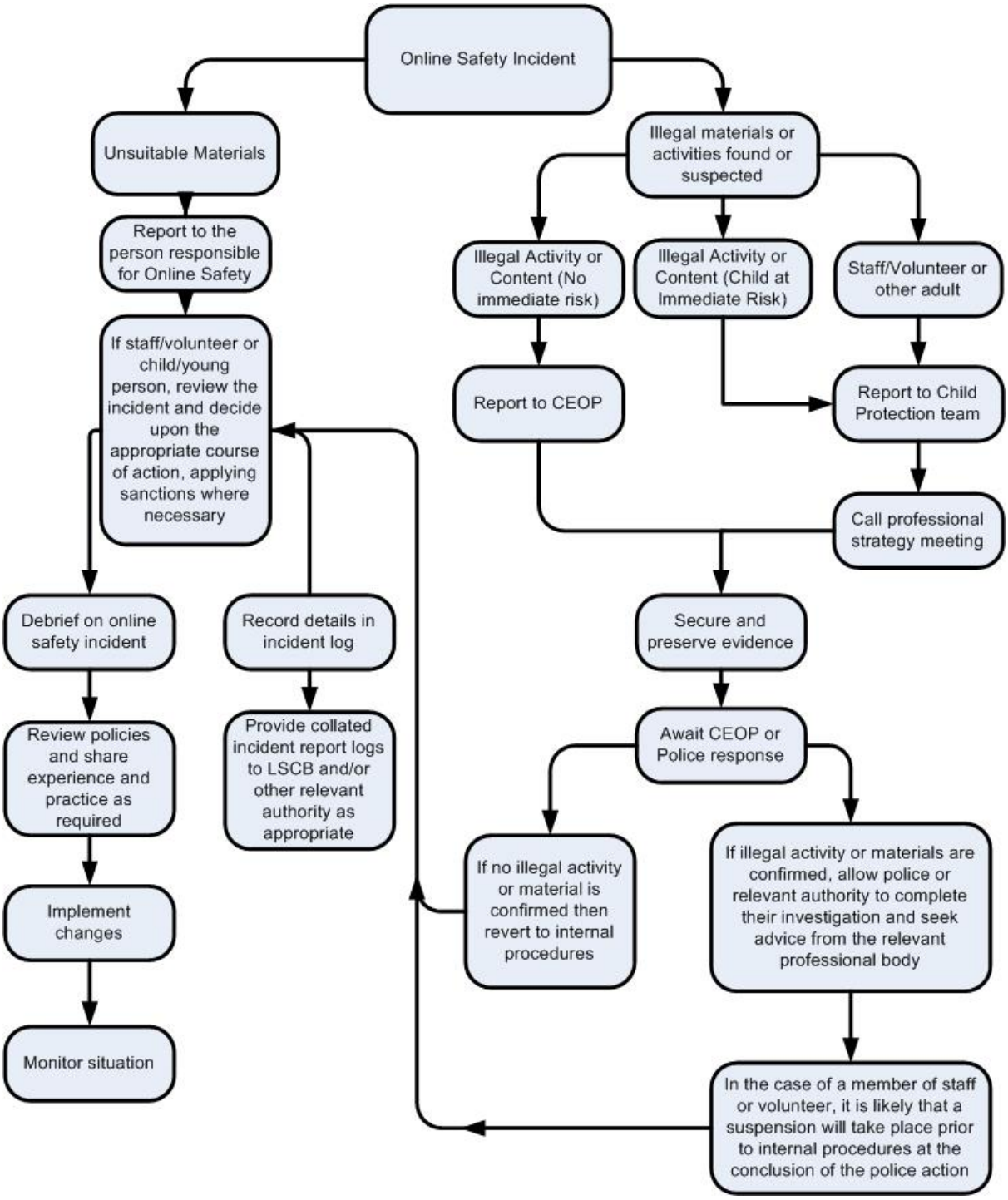
- No reference should be made in social media to students, parents or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Social Media incidents re: students.

- Incident is investigated by appropriate staff – in most cases e-safety designated person – ***L Fletcher, N Dunbar, Z Fox***
- Device is confiscated as per Searching and Screening Policy and e-safety content recorded and removed. If designated staff are re-assured then device is returned.
- e-Safety / social media discussion is undertaken to ensure the child understands the impact and their responsibility on line.
- If appropriate, sanctions are imposed as per School Behaviour Policy.
- Device is confiscated until parents collects
- Incident recorded on e-safety log and e-safety letter sent home (appendix 1)

Illegal or Inappropriate Activity

If there is any suspicion that a child or adult at Our Lady's is involved in illegal or inappropriate activity on line or social media the following incident flow chart will be followed alongside school safeguarding procedures for the safety of the victim.



Other Incidents

It is expected that all members of the school community will be responsible users of digital technologies, who understand and follow school 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 of serious misuse of digital technologies, all steps in this procedure should be followed:

- Have more than one senior member of staff 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.
- 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 / Academy Group 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
    - promotion of terrorism or extremism
- Isolate the computer in question as quickly as possible. 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 safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Approved Jan. 2019

Appendix 1

Dear Parent/Carer

E-Safety Incident Information

Your child, ……, has been involved in a negative e-safety incident using social media, which has resulted in another child/children being upset and the school having to conduct an investigation. You should have received a phone call about this. If this is not the case, the incident relates to:

……..

This incident has been recorded in our central e-safety record. Please can you take the time to read the guidance below and speak to your child regarding the incident and their future online activity.

The internet has become an integral part of children's lives, enabling them to undertake research for school projects, talk to their friends and access information from around the world. Increasing provision of the internet in and out of school brings with it the need to ensure that students are safe.

Social media development is constantly evolving into ever more innovative areas with many apps enabling amazing creativity and interaction between peers.

Unfortunately, however, there are times when social media use can have a negative impact on children. Parents should be aware of the potential dangers by taking measures to ensure safe usage by all. The terms and conditions for all social media sites, including Facebook, Instagram and Snapchat state that a child must be aged 13 to have an account. The age 13 is linked to the maturity of a child to deal with this level of communication, interaction and the potential dangers. Therefore, if your child is experiencing problems on these sites and they are not 13, it is very difficult for the school to help resolve them. It is our advice that you adhere to the terms and conditions provided by the companies and not allow your child to create an account.

As a Catholic school, we are fully committed to resolving any pastoral issues that we may encounter with the help of our strong pastoral team. If your child is responsible for causing a negative e-safety experience for another child/children then the incident will be logged in our central e-safety record along with the details. If necessary, we will share this record with the police.

If you require any further details or support please contact either Mrs Fletcher or Mr Dunbar via the email addresses shown below.

Yours sincerely

L Fletcher *N Dunbar*

Mrs L Fletcher (Subject Leader of ICT)
Director of Targeted Pastoral Support
l.fletcher@olqp.lancs.sch.uk

Mr N Dunbar (Assistant Headteacher)
Designated Safeguarding Officer
n.dunbar@olqp.lancs.sch.uk

Updated and approved October 2019