Our Lady's Catholic College
Online Safety Policy
(including KCSIE 2023 monitoring and filtering action plan)

Last updated	September 2023
Approved by the governing body	Autumn 2023
Date to review	September 2024

Context

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; for example pornography, fake news, racist or radical and extremist views;
- contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- conduct: personal online behaviour that increases the likelihood of, or causes, hark; for example making, sending and receiving explicit images, or online.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The school online policy will help to ensure safe and appropriate use. The development and implementation of the policy will involve all the stakeholders in a child's education from the Headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves. Broughton has robust safeguarding procedures in place and understands that online safety is an integral part of keeping children safe. Keeping Children Safe in Education 2022.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- Risk of radicalisation through social media and the use of the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Online bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional well-being and development and learning of the young person

Many of these risks reflect situations in the off-line world and it is essential that this online policy is used in conjunction with other school policies (e.g. Behaviour, including anti-bullying, and safeguarding/child protection policies).

As with all other risks, it is impossible to eliminate those concerns completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school will demonstrate that it has provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected, to manage and reduce these risks. The Online Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in

order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
Our Lady's online safety policy reflects the importance it places on the safe use of information systems and electronic communications. Online safety encompasses not only internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.

- Online safety concerns safeguarding children and young people in the digital world.
- Online safety emphasises learning to understand and use new technologies in a positive way.
- Online safety is less about restriction and more about education about the risks as well as the benefits so we can feel confident online.
- Online safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

The internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networks all transmit information using the internet internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the internet make it an invaluable resource used by billions of people every day.
Some of the material on the internet is published for an adult audience and can include violent and adult content. Information on weapons, crime, racism, extremism and radicalisation may also be unsuitable for children and young people to access. Pupils need to develop critical skills to evaluate online material and learn that publishing personal information could compromise their security and that of others. Schools have a duty of care to enable pupils to use on-line systems safely.
Our Lady's Catholic College needs to protect itself from legal challenge and ensure that staff work within the boundaries of professional behaviour. The law is catching up with internet developments: for example, it is an offence to use email, text or instant messaging (IM) to 'groom' children.
It is the responsibility of the school to make it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised" and ensure an Acceptable Use Policy is in place.
Online safety training is an essential element of staff induction and part of an ongoing CPD programme.
The rapid development and accessibility of the internet and new technologies such as personal publishing and social networking means that online safety is an ever growing and changing area of interest and concern. The school's online safety policy reflects this by keeping abreast of the vast changes taking place around us.
This policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.
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 online bullying, or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.
* This policy runs in conjunction with the 'Social Networking Sites and Social Media Policy'.

Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports as part of Headteacher's termly report.

The nominated Safeguarding Governor has taken on the role of Online Safety Governor

The role of the Online Safety Governor will include:

- Liaising with Online Safety Designated person
- Reporting to relevant Governors committee / meeting

Headteacher and Senior Leaders:

- The Head teacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Designated person
- The leadership team members are responsible for ensuring that the Online Safety Person and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant
- A member of the Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles (network filtering supervision, appropriate use of IT consent for pupils and spot checks for example).
- The Head teacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see Appendix 1 - flow chart on dealing with online safety incidents)

Online Safety Designated person:

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place, including recording of incidents on CPOMS.
- Organises training and advice for staff.
- Liaises with the Local Authority.
- Liaises with school ICT technical staff and Head of Computing
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- Liaises with Online Safety Governor to discuss current issues
- Attends relevant meeting / committee of Governors
- Reports regularly to Senior Leadership Team

Network Manager:

The Network Manager is responsible for ensuring:

- The school's ICT infrastructure is secure and is not open to misuse or malicious attack
- The school meets the online safety technical requirements outlined in the school's Acceptable Usage Policy and any relevant Local Authority Online Safety guidance
- Users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- The school's filtering procedure is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- They keep up to date with e-safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- The use of the network / Virtual Learning Environments (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Designated person for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school procedures.

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- They report any suspected misuse or problem to the Online Safety Designated person / ICT Co-ordinator/Network Manager for investigation / action / sanction via Technical Services / record on CPOMS if appropriate.
- Digital communications with pupils (email / Virtual Learning Environment (VLE)) should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils understand and follow the school online safety and acceptable use policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned pupils should 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

Designated person for child protection

Should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Online bullying
- Online materials related to extremism and radicalisation
- Have an understanding of "the filtering and monitoring systems and processes in place

Pupils:

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking / use of images and online bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local online safety campaigns / literature. Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy

Education – How pupils are taught to keep themselves safe

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks including exploitation and extremism and build their resilience to these risks.

Online safety education will be provided in the following ways:

- A planned online safety programme should be provided as part of ICT / CPSHE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key online safety messages should be reinforced as part of a planned programme of assemblies.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems / internet will be posted in all rooms.
- Pupils should adhere to rules regarding phone use in school: to be out of sight before pupils enter the school site and only to be accessed again after 3pm outside of the school building.

Education – Parents / Carers

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 experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, Broughton website, VLE
- Parents' evenings

Education & Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Online safety training will be made available to staff.
- Staff are familiar with the guidance related to Online Safety in Keeping children safe in education 2022
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies
- The Online Safety Designated person will receive regular updates from the Head of ICT/IT Technicians through attendance at LA / other information / training sessions and by reviewing guidance documents released by the local authority and others.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The Online Safety Designated person will organise the provision of advice / guidance / training to individuals as required

Training – Governors

- Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any committee / group involved in ICT / online safety / health and safety / child protection. This may be offered in a number of ways:
- Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation.

Technical – infrastructure / equipment, filtering and monitoring

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 ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Technicians
- All users will be provided with a username and password by (Technicians) who will keep an up to date record of users and their usernames.

- The “master / administrator” passwords for the school ICT system, used by the Technicians must also be available to the Headteacher and Online Safety Designated person.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- In the event of the Technicians needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher and/or the Online Safety Designated person.
- Requests from staff for sites to be removed from the filtered list will be considered by the Technicians.
- School ICT technical staff monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place for users to report any actual / potential online safety incident (CPOMS / CEOP / Report Harmful content / Report-remove/ Smoothwall)
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of “guests” (eg. trainee teachers, visitors) onto the school system.
- An agreed policy is in place that restricts staff from installing programmes on school workstations / portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.

Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should 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 pupils are allowed to freely search the internet, eg. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils 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 technicians 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.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils will not be permitted to use their mobile phone in class unless permission has been granted in advance from the Headteacher.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. 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 should inform and educate pupils 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.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Parents or carers will have the option to opt in for any photographs of pupils which are to be used for educational or marketing purposes.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.When personal data is stored on any portable computer system, USB stick or any other removable media:
- The data must be encrypted and password protected
- The device must be password protected
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete
- The device must offer approved virus and malware checking software

Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg. by remote access).
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Web-based technologies

- The Internet provides instant access to a wealth of up-to-the minute information and resources from across the world, which would not ordinarily be available.
- Use of email enables improved communication and facilitates the sharing of data and resources.
- Virtual Learning Environments (VLEs) provide pupils with a platform for personalized and independent learning.

Risks

- Pupils might inadvertently access content of an unsavoury, distressing or offensive nature on the Internet or receive inappropriate or distasteful e-mails.
- Pupils might receive unwanted or inappropriate e-mails from unknown senders, or be exposed to abuse, harassment or online bullying via e-mail, text or instant messaging,in chat rooms or on social-networking websites and apps, such as Facebook, Whatsapp,Instagram etc.
- Chat rooms provide cover for unscrupulous individuals to groom children.
- Identify theft (including hacking Facebook profiles)

Procedures for use for use of a shared network

- Users must access the network using their own accounts. These must not be disclosed or shared.
- Users must respect confidentiality and attempts should not be made to access another individual's account or files on the network without permission.
- Software should only be installed by the ICT Technician.
- Users must ensure they have adequate virus protection on any machine on which they use removable media before it is used in school.
- Machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.' (Ctrl+alt+del followed by 'lock computer').
- Machines must be 'logged off' correctly after use.

Procedures for use of the internet and email

- All users must sign an 'Acceptable Use Agreement' before access to the Internet and email is permitted in the establishment.
- Users must access the Internet and e-mail using their own account and not those of another individual. Passwords must remain confidential and no attempt should be made to access another user's e-mail account. If you feel your account details are known by others you should change your password immediately.
- The Internet and e-mail must be used in a reasonable manner adhering to the professional judgment of the supervising member of school staff.
- Pupils must be supervised at all times when using the Internet and e-mail in school.
- Procedures for safe Internet use and sanctions are applicable if rules are broken.
- Internet and e-mail filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk or unwanted correspondence. This is to be reviewed and updated regularly.
- Internet and e-mail use will be monitored regularly in accordance with the Data Protection Act 2018.
- Users must be careful when they disclose any information of a personal nature in an e-mail or on the Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified.
- All e-mails sent should be courteous and the formality and tone of the language used appropriate to the reader. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- Bullying, harassment or abuse of any kind via e-mail will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- If users are bullied, or offensive e-mails are received, this must be reported immediately to a trusted adult or member of staff within the service / establishment. emails received should not be deleted, but kept for investigation purposes.
- Copyright must not be broken.

File transfer:

Files may be taken home or brought into school by pupils by using One Drive. Remember - the school uses special filtering software, which prevents you from accessing most unsuitable sites and it also records every attempt you make to hit a site, whether successful or not, when and where you did it and who you are. So remember - every action you take under your account is recorded, and may be accompanied by screenshots and/or recordings of your session.

Procedures for use of cameras, digital photos and webcams and any other digital device

- Permission must be obtained from a pupil's parent or carer before photographs or video footage can be taken.
- Photographs and/or video footage can be downloaded and stored into an appropriate area under the guidance of the Network Manager.
- Any photographs or video footage stored, must be deleted immediately once no longer needed.
- Pupils and staff must conduct themselves in a polite and respectful manner when representing the school in a video conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation. Procedures to ensure safety of Our Lady's Catholic College website
- All content and images must be approved before being uploaded onto the website prior to it being published.

- The website is checked every term to ensure that no material has been inadvertently posted, which might put pupils or staff at risk.
- Copyright and intellectual property rights are respected.
- Permission is obtained via the data collection sheet from parents or carers before any images of pupils can be uploaded onto the website.
- When photographs to be used on the website are saved, names of individuals should not be used as file names.

Procedures for using mobile phones, digital and other devices

- The school is NOT responsible for pupils' personal mobile technology damaged, lost or stolen. Items are brought to school at your own risk.
- If a mobile phone, or any other digital device needs to be brought into school, it should be switched off at all times and stored away.
- If a mobile phone or another device is activated in school when not directed by the teacher as part of a lesson, it will be confiscated immediately, recorded and handed in at Pupil reception. A sanction will apply.
- Staff will not copy/distribute/view images on any pupils' personal mobile device.
- The use of games consoles will not be permitted in school at any time. Pupils may use e- readers (e.g. Kindles) as part of literacy developments and other e-reading.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Online terrorist and extremist material
- Other criminal conduct, activity or materials

If a pupil breaks any of the rules, consequences could be:

- A temporary ban on the use of all computer facilities at school until a discussion takes place with the Head of Computing and/or a Senior Leader, Head of Year.
- A ban, temporary or permanent, on the use of the internet facilities at school.
- Appropriate punishment within the departmental and/or school pastoral systems.
- A letter informing parents what has occurred.
- Referral to Channel, part of Prevent strategy
- Contact with the Police, depending on the nature of the image and the age of the people involved.
- Any other action decided by the Headteacher and Governors of the school.
- The flow chart in Appendix 1 should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

Training

- All staff and pupils to receive regular and up-to-date training via CPSHE, Computing and within departments for pupils. INSET provision will be provided for school based staff.
- Pupils will receive age appropriate online safety information within the school curriculum which focusses on how to stay safe, protect themselves from harm and how to take responsibility for their own online safety and that of others.

KCSIE 2023 Filtering and monitoring action plan (taken from KCSIE 2023 OLCC action plan)

1. **Identify a member of the senior leadership team and a governor, to be responsible for ensuring these standards are met**. JLX(DSL) / PJ (Chair of Governors) to have overall responsibility, ensuring accountability and half termly updates on new software and updates.
2. **Set out the roles and responsibilities of staff and third parties (as above), external service providers.**
    - Smoothwall connect- digital monitoring works in real-time to alert safeguarding teams to risks as they happen. Helps prevent online risks becoming real-life incidents. Meets all requirements for proactive / appropriate monitoring. Captures user activity as it happens, automatically sending potential risks through to the Monitor portal. Captures activity that may indicate a risk, even outside of the regular web browser such as in a Word Document, Messaging app, or encrypted "dark web" browser. 24/7 in-house team of moderator's review captures to minimise false positives and contact you by phone for any urgent risks. Alerts are sent in real-time by phone, email, and stored within the intuitive portal for you to review. Integrates with CPOMS. Allowing DSL to respond to risk real time, putting in appropriate support.
    - Local authority – fire wall and filter, daily report overseen by network manager intervened and reported concerns to head teacher and DSL as appropriate.
3. **Schedule half termly review of filtering and monitoring provision.** JLX/DSL/ SS meet with updates from LA and Smoothwall, ensuring we are reducing the risk to the highest degree. Identifying the actions taken from alerts and evaluating our procedures.
4. **Undertake tests now to ensure harmful and inappropriate content has been blocked without impacting teaching and learning.** Smoothwall has real time Captures activity that may indicate a risk, even outside of the regular web browser such as in a Word Document, Messaging app, or encrypted "dark web" browser. Direct contact made to school based on prioritisation.
5. **Report to governing body the efficacy of monitoring strategies in place**. Termly agenda item, as part of safeguarding up date to 'communities' meeting and Chair of Governors.

Schedule for Development / Monitoring / Review

This online safety policy was approved by the Governing Body / Governors' Access and Support Committee on: awaiting approval

The implementation of this online safety policy will be monitored by: SLT

Monitoring will take place at regular intervals: annually

The Governing Body / Governors Sub Committee will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at half termly intervals

The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be: September 2024

Should serious online safety incidents take place, the following external persons / agencies should be informed:

Lancashire Safeguarding Children Board

Tim Booth (LADO)

(01772) 536694

tim.booth@lancashire.gov.uk
Online Safety Contact
Concluding statement:
The procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in the technology at Our Lady's Catholic College. It may be that staff /pupils might wish to use an emerging technology for which there are currently no procedures in place. The use of emerging technologies will be permitted upon completion and approval of a risk assessment, which will be used to inform future policy

Appendix 1

<table>
<tr><th colspan="4">Online Incident</th></tr>
<tr><th colspan="3">Involving students
Member of staff assess severity according to OLCC Policy then:</th><th>Involving member of staff</th></tr>
<tr>
<td>Low Severity
For example:
Misuse of school email system, off task on internet

Member of staff follows procedures from OLCC Behaviour Policy

Logs incident on synergy</td>
<td>Medium severity
For example:
inappropriate sites, bypass filters, playing games without permission

Report to network manager and Behaviour lead

Logs incident on synergy

Logs incident on CPOMS as 'internet misuse' follows procedures from OLCC Behaviour Policy

Account and/or internet may be disabled

Supplementary user agreement issued, parents /student sign and return</td>
<td>High severity
For example, abuse about staff, misuse of school email system for bulling, cyber bullying, inappropriate images.

Report to network manager and Behaviour lead via synergy, discussion with PSO, PL, Head of ICT, Head teacher, DSL and decide appropriate course of action.

Account disabled until further notice

Meeting with parents

May be necessary to report to other agencies such as police , MASH, Channel</td>
<td>For example.
Inappropriate sites including social networking

Report to Head teacher directly who will decide on appropriate course of action</td>
</tr>
</table>