Our Lady's Catholic College

Online Safety Policy

September 2017

Contents

Principles of the Policy

At Our Lady's Catholic College we teach young people about how to form relationships, including understanding loving relationships and acknowledging that young people's first experience of love is in the home. We encourage the young people in our school to recognise that they are all children of God and that each person shares a God given dignity.

Online technologies play a huge role in modern life and developing relationships so providing a broad and balanced online safety education at each key stage is vital to ensuring that students can navigate the online world safely and positively. Online safety is interwoven into many aspects of our curriculum and written with the HSRE 2017 policy and curriculum in mind. This policy sets out our aim to keep our students and staff safe whilst online.

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by Stephanie Bell, Online Safety Officer, and a student working group; OLCC Digital Leaders.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body:	*July 2017*
The implementation of this Online Safety policy will be monitored by the:	*Online Safety Officer, SLT, OLCC Digital Leaders*
Monitoring will take place at regular intervals:	*Yearly*
The Governing Body receive a report on the implementation of the Online Safety Policy generated by the monitoring group at regular intervals:	*Yearly*
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:	*Summer Term 2018*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer, LADO, Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students
    - parents / carers
    - staff

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities 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. The Safeguarding Governor is also responsible for Online Safety. The role of the Online Safety Governor will include:

- receive regular reports from the Online Safety Officer as part of the Safeguarding meetings
- reporting to Pupil Well Being committee

Headteacher and Senior Leaders:

- The Headteacher has a duty of care 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 Officer.
- The Headteacher and Deputy Headteacher 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.
- The Headteacher/Senior Leaders are responsible for ensuring that the Online Safety Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher/Senior Leaders 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.
- The SLT will receive regular monitoring reports from the Online Safety Officer.

Online Safety Officer in coordination with Lead DSL:

- Leads the OLCC Digital Leaders student group.
- Chairs the Online Safety Group
- Advises the Pastoral Team with online safety issues and makes an anonymous record of the incidents to inform future online safety developments.
- 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.
- Provides training and advice for staff
- Liaises with the Local Authority / relevant body
- Liaises with school technical staff
- Reports regularly to SLT

Designated Safeguarding Lead (DSL) & Deputy DSL:

Should be trained in Online Safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying

Network Manager / Technical staff:

The Network Manager / Technical Staff are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network, internet, Learning Platform, remote access and email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

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 Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Headteacher or member of the Senior Leadership Team for investigation/action/sanction
- all digital communications with students/parents/carers 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 activities
- students understand and follow the Online Safety Policy and Acceptable Use Policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- if unsuitable material is (unintentionally) found by a student that URL (web address) is reported to the Network Manager/IT Technician to be block. If a student intentionally finds unsuitable material the URL is reported to the Network Manager/IT Technician and the Behaviour Policy is referred to for the sanction.

Students:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on 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 and carers will be encouraged to support the school in promoting good online 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 online student records
- their children's personal devices in the school (where this is allowed)
- encourage their child to use technology responsibly and safely

Online Safety Group

The Online Safety Group is a group with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. They will meet once a term and report to SLT and the Pupil Welfare Committee. Members of the Online Safety Group will assist the Online Safety Officer with:

- the production / review / monitoring of the school Online Safety Policy / documents.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents/carers and the students about the online safety provision

Members of the group will include:

- Online Safety Officer (chair)
- Member of SLT with safeguarding responsibility (DSL or Deputy DSL)
- Network Manager or IT Technician
- Member of the OLCC Digital Leaders group (Pupil Voice)
- Pastoral Leader
- Pastoral Support Officer (PSO)
- Member from the Governors Pupil Welfare Committee

Policy Statements

Education – Students

Students need the help and support of the school to recognise and avoid online safety risks and build their resilience. Online safety should be 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 should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students should be helped to understand the need for the Student Acceptable Use Agreement and SHINE Online rules to adopt safe and responsible use both within and outside school.
- Staff should 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 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 students are allowed to freely search the internet, 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, 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 can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be emailed to the IT Technicians and a log made of the request.

Education – Parents / Carers

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

- Curriculum activities
- Letters, newsletters, website, OLCC Facebook page & OLCC Digital Leaders Facebook page.
- Parent /Carers evenings/sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g., swgfl.org.uk, www.saferinternet.org.uk, http://www.childnet.com/parents-and-carers

Education & Training – Staff/Volunteers

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:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- 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 Agreements.
- It is expected that some staff will identify online safety as a training need within the Appraisal process.
- The Online Safety Officer will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

Governors / Directors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school 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 technical systems will be 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 must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the IT Technicians 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 90 days.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager and IT Technician must also be available to the Headteacher or Deputy Headteacher and kept in a secure place (e.g. school safe)
- 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. There is a clear process in place to deal with requests for filtering changes; staff email the request and a log of the request is kept.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different groups of users – staff / students etc.)
- School technical staff regularly monitors and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place staff email the request and a log of the request is kept for users to report any actual / potential technical incident / security breach to the IT Technicians.
- Appropriate security measures are in place 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.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. Supply usernames and password for external "guests" copy of the Staff AUP in the supply staff pack.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Encrypted pen drives available from the IT Technicians.

Data Protection

Covered in Data Protection Act Policy

Communications

When using Office 365 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. Users should be aware that email communications are monitored.
- Users must immediately report, to the Online Safety Officer – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content.

Social Media - Protecting Professional Identity

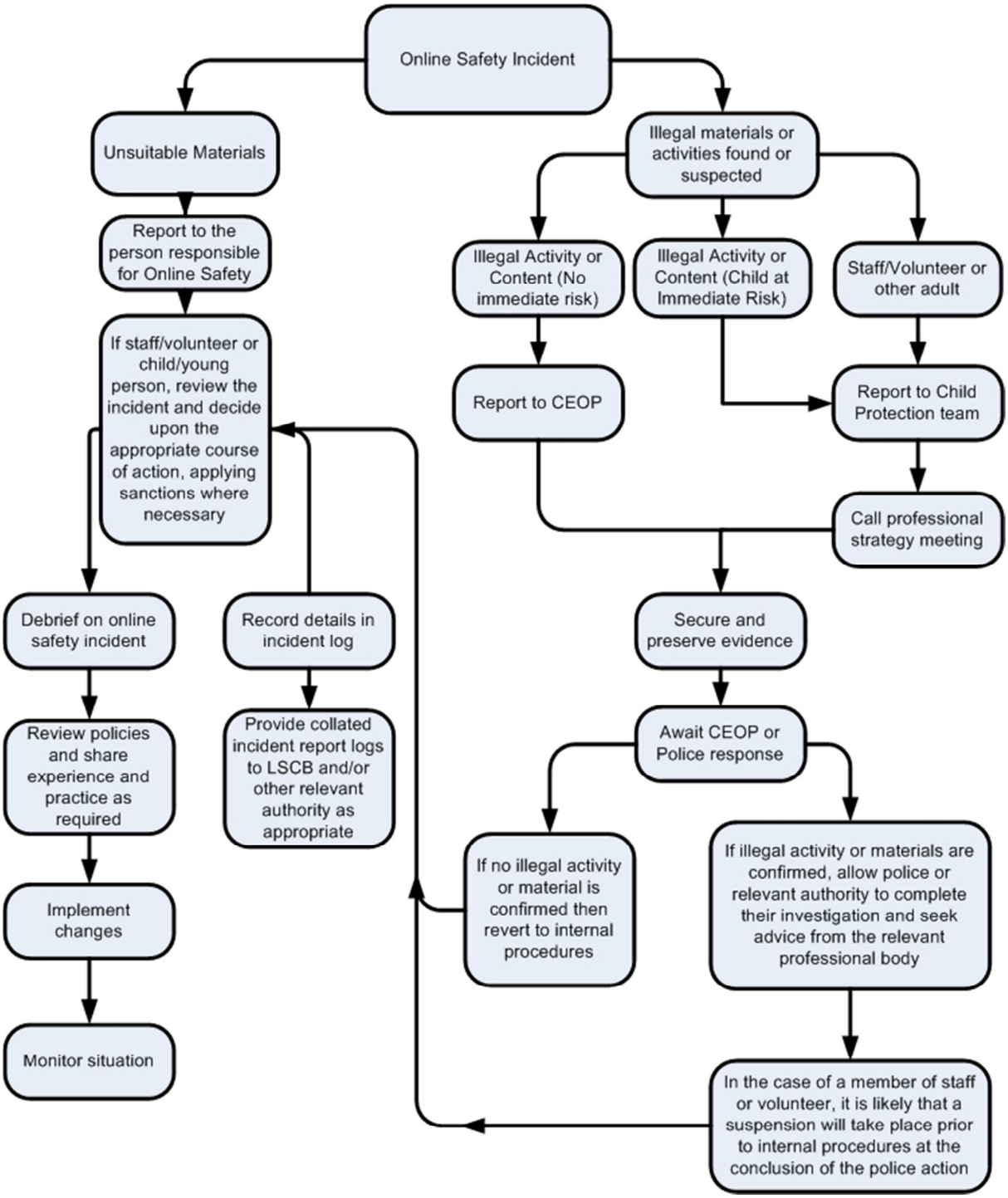
Covered in Social Networking Sites and Social Media - Policy - Feb 2016

Unsuitable / inappropriate activities

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	

Illegal Incidents Flowchart

If there is any suspicion that the website(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 for responding to online safety incidents and report immediately to the police.



School Actions & Sanctions

Nature of behaviour	First Offence	Repeat Offences	Logged as 'type'
Deliberately accessing or trying to access material that could be considered illegal	Refer to Headteacher/SLT/DSL Refer to Police or other agencies Online Safety Officer notified Parents/carers informed Removal of network/internet access rights FTE/Permanent Exclusion		Online Safety - illegal
Unauthorised use of non-educational sites during lessons	Use of class procedure		Steps 3, 4 or 5
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	Phone confiscated. Returned back after 60 min detention, that night, in the SLT detention.		Mobile Phone
Unauthorised / inappropriate use of social media / messaging apps / personal email	Use of class procedure Notify IT Technicians of web address to restrict		Steps 3, 4 or 5
Unauthorised downloading or uploading of files	Warning Notify IT Technicians	Refer to Subject Leader or Pastoral Leader 60 min Detention	Network Rule
Attempting to access or allowing others to access school network by sharing username and passwords	Warning	30 min Subject Teacher detention	Network Rule
Attempting to access or accessing the school network, using the account of a member of staff	SLT detention Online Safety Officer notified Headteacher/SLT notified	Exclusion Unit	Network Rule - serious
Corrupting or destroying the data of other users	Refer to Subject Leader 60 min detention	SLT detention	Network Rule
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature using Office 365 to a student	SLT detention Parents/carers informed Online Safety Officer notified	Exclusion Unit Removal of network/internet access rights (length of ban to be agreed by SLT)	Bullying
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature using Office 365 to a member of staff	1 day exclusion unit Removal of network/internet access rights (length of ban to be agreed by SLT)	1-5 days exclusion unit Removal of network/internet access rights (length of ban to be agreed by SLT)	Staff – offensive email
Actions shared online which could bring the school into disrepute or breach the integrity of the ethos of the school	Refer to Headteacher/SLT SLT detention Exclusion Unit FTE Parents/carers informed Online Safety Officer notified		Online Safety – ??
Using proxy sites or other means to subvert the school's filtering system	Use of class procedure Notify IT Technicians of web address to restrict		Steps 3, 4 or 5
Accidentally accessing offensive or pornographic material and failing to report the incident	Warning Parents/carer informed Online Safety Officer notified IT Technicians notified	SLT detention	Online Safety – accidental offensive material
Deliberately accessing or trying to access offensive or pornographic material	SLT Detention Refer to SL and/or PL Removal of network/internet access rights (length of ban to be agreed by SLT) Parents/carer informed Online Safety Officer notified	Exclusion Unit Extended removal of network/internet access rights (length of ban to be agreed by SLT) Parents/carer informed	Online Safety – deliberate offensive material
Plagiarism/infringement of copyright in assessment work	Refer to SL Work to be redone in detention Parents/carer informed	Refer to PL and/or ASM Refer to exams officer Parent/carer informed	Plagiarism
Nude Selfie incident (requesting or sharing – *NOT the creator of the image*)	Refer to Headteacher/SLT Refer to DSL & Pastoral Team Refer to Lancashire Safeguarding Board and/or Police Online Safety Officer notified Parents/carers informed		Online Safety - sexting

Appendix

Students Acceptable Use Policy Agreement

Rules for responsible internet use at OLCC

This computer system and the Network are owned by the school and is monitored including websites and e-mail. Any unlawful text, imagery, sound or material deemed inappropriate will be deleted. Any criminal activity on the network will be reported. ICT system security must be respected and no attempt should be made to bypass any security or restrictions enforced by either the school or county servers.

1. Only use your own login and password, keep it confidential.
2. Only use the Internet when there is a teacher or adult present to supervise or when you have been given specific permission.
3. Only use the Internet for school based purposes.
4. Ask an adult if you are unsure that a web source is reliable and the information you are going to use is accurate.
5. Reference websites that you use in your work, copyright and intellectual property rights must be respected
6. Downloading and storage of media files is forbidden e.g. MP3, WMA files
8. Ask permission from a member of staff before using web-based e-mail.
9. E-mails should be polite, appropriate and sensible if you receive a rude or offensive message report it to a teacher immediately.
10. Never give out your address, phone number or arrange to meet someone over the Internet
11. If you see anything offensive or you feel uncomfortable about anything, report it.
12. The use of chat rooms or Social networking sites is strictly prohibited.
13. Use of the Internet for personal financial gain, gambling, political purposes or advertising is not permitted.

By signing this you are agreeing to the Terms and Conditions stated in this policy.

You will also be agreeing to this every time you log on and click ok.

Signed:_____

Date:_____

Staff (and Volunteer) Acceptable Use Policy Agreement

OLCC Staff Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I will not allow a student to use my account under any circumstances. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within reason.
- I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, DSL, Online Safety Officer or IT Technician – where appropriate.

I will be professional in my communications and actions when using school ICT systems:

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students and parents/carers using official school systems, Office 365. Any such communication will be professional in tone and manner.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted.
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted and kept secure.
- I understand that Data Protection Policy requires that any staff or students data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software to the IT Technicians.

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

Responding to Nude Selfie/Sexting Incidents

Pan-Lancashire LSCB Online Safeguarding Group

Sexting in Schools & Colleges: Flowchart for responding to incidents

The flowchart process below is directly taken from the *Sexting in schools & colleges: Responding to incidents and safeguarding young people* guidance produced on behalf of the Government by the UK Council for Child Internet Safety (UKCCIS). It highlights the jointly-recommended process advocated by Lancashire and Blackburn with Darwen Safeguarding Boards in partnership with Lancashire Constabulary for managing and responding to Sexting incidents and includes additional annotations to signpost useful supporting resources and a number of Frequently Asked Questions.

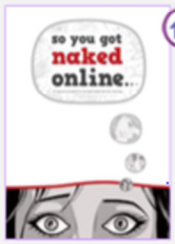
Supporting Resources

Highly Recommended

Nationally-recognised best-practice guidance for Schools & Colleges. It is strongly recommended that **all Designated Safeguarding Leads (DSLs) should be expressly familiar with this guidance**

Online Safety Helpline: Highly-recommended helpline for professionals working with Children & Young People seeking further advice and support with online issues

Support For Young People: Practical post-incident advice from SWGfL to support Young People



Curriculum delivery: Excellent Key Stage 2 NSPCC Teaching Resources including videos *'I Saw your Willy'* and *'Lucy and the boy'*

Highly Recommended

Curriculum delivery: Very useful PSHE curriculum resource for 11-14 y/o covering a variety of Online Safety areas including Sexting

UKCCIS Flowchart for responding to Sexting incidents

Initial disclosure: This could come from a pupil directly, a parent, a pupil's friend.

Initial review with safeguarding team: At this initial stage the safeguarding team review the information and consider the 5 points for immediate referral. They make an initial decision about **whether the incident can be dealt with in house.** (For more information see page 13 of UKCCIS Sexting in schools and colleges)

Risk assessment / Dealing with the incident: Consider the risk of harm and at any point if there are 'causes for concern' you can refer back to police/social care. (For more information refer to page 14 and Annex A of UKCCIS Sexting in schools and colleges)

Management in school: Ensure parents are informed and the incident recorded **following all child protection and safeguarding procedures.** (For more information see page 14 of UKCCIS Sexting in schools and colleges)

UKCCIS guidance

5 points for referral:
1. **Adult involvement**
2. **Coercion or blackmail**
3. **Extreme or violent**
4. **Under 13**
5. **Immediate risk of harm**

(For more information refer to section 2 of UKCCIS Sexting in schools and colleges)

LSCB Supporting note: If the incident meets the criteria for Police referral, reporting should focus on **describing** rather than **diagnosing** the incident

Police / Social Care / MASH referral
Refer to your local arrangements for dealing with incidents and contact local services. (For more information refer to page 17 of UKCCIS Sexting in schools and colleges)

UKCCIS guidance

Considerations – Risk Assessment
-Vulnerability of the child
-Coercion
-How shared and where
-Impact on children
-Age of the children
(For more information see UKCCIS Sexting in schools and colleges - Annex A)

LSCB Supporting note: Incident review arrangements may include reviewing curriculum provision

Lancashire Safeguarding Boards · Blackburn with Darwen · Lancashire Constabulary

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy:

UK Safer Internet Centre
Safer Internet Centre – http://saferinternet.org.uk/
South West Grid for Learning - http://swgfl.org.uk/

Childnet – http://www.childnet-int.org/

Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline

Internet Watch Foundation - https://www.iwf.org.uk/

CEOP - http://ceop.police.uk/

ThinkUKnow - https://www.thinkuknow.co.uk/

INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm

UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis

Netsmartz - http://www.netsmartz.org/

Online Safety BOOST – https://boost.swgfl.org.uk/

360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

Bullying / Cyberbullying

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388

DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – new Cyberbullying guidance and toolkit (Launch spring / summer 2016) - http://www.childnet.com/new-for-schools/cyberbullying-events/childnets-upcoming cyberbullying-work

Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks
SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people
Connectsafely Parents Guide to Facebook
Facebook Guide for Educators

Curriculum
SWGfL Digital Literacy & Citizenship curriculum

Glow - http://www.educationscotland.gov.uk/usingglowandict/

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Mobile Devices / BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking

NEN - Guidance Note - BYOD

Working with parents and carers
SWGfL Digital Literacy & Citizenship curriculum
Online Safety BOOST Presentations - parent's presentation
Connectsafely Parents Guide to Facebook
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops / education
The Digital Universe of Your Children - animated videos for parents (Insafe)
Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
Insafe - A guide for parents - education and the new media
The Cybersmile Foundation (cyberbullying) - advice for parents

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011
Futurelab - "Digital participation - its not chalk and talk any more!"
Ofcom – Children & Parents – media use and attitudes report - 2015

Glossary of Terms

AUP	Acceptable Use Policy
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.