eSafety Policy

Introduction

This policy is available for parents, staff, and pupils to access. Rules relating to the school code of conduct when online, and e-safety guidelines, are displayed around the school. E-safety is integrated into the curriculum through Using ICT, subjects areas *and during PSHE lessons where personal safety, responsibility, and/or development are being discussed. The policy should be read in conjunction with the Acceptable Use Policy, Child Protection Policy, Behaviour Policy, Pastoral Policy, Anti-Bullying Policy and Data Protection Policy.*

The college has a duty of care to enable pupils to use on-line systems safely. eSafety (electronic safety) is the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. The eSafety Policy refers not only to Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. Since ICT is a compulsory cross-curricular element of the curriculum, eSafety learning is built into the delivery of the curriculum itself.

eSafety in the school context is concerned with safeguarding children and young people in the digital world; while it emphasises learning to understand and use new technologies in a positive way, it also focuses on education about the risks as well as the benefits so that users feel confident online. eSafety is concerned with supporting pupils to develop safer online behaviours both in and out of school and helping them recognise unsafe situations and how to respond to risks appropriately.

The e-safety policy covers the use of the computing systems, equipment and software in school. It also covers the use of school-owned technology outside school and the use of personal technology in school. The college is committed to act on e-safety incidents outside the school that affect the well-being of staff and pupils within the school by referring incidents to the PSNI where appropriate.

Curriculum Provision

Pupils are prepared within the curriculum to need to learn to recognise and avoid risks such as exploitation on the internet — to become “Internet-wise” and ultimately good “digital citizens”. The taught ICT programme provides direct eSafety learning at KS3. The college’s PTA arranges for biennial presentations on eSafety to pupils and parents through the PSNI and school’s Head of E-Learning. Year 8 pupils will receive an induction session pertaining to the use of the C2K network and the College’s AUP.

Care will be taken when making use of social media for teaching and learning and each social media technology that is to be utilised should be risk assessed in the context pupil age, appropriateness of content and relevance to the curricular requirements of the course.

Use of social media sites in school will be for teaching purposes only and under the supervision of staff at all times. Teachers planning to make use of social media sites within the classroom will have risk assessed the materials and content in advance and checked with the Head of Department that the material is suitable for use. Use of live or real time sites raises particular concerns for children and young people, and will only be used by teachers if necessary and with due diligence.

C2k and school eSafety

While C2k provide a filtering service on managed technology within school, no filtering service can provide 100% security. The managed C2k systems within the college are monitored and the principal will, upon request, be provided with security reports from C2k on usage by any member of staff or pupil in the college. Pupil access to sites are limited to those deemed "green" by C2k and any "grey filtered" access will be provided only under direct staff supervision for the purpose of curriculum teaching and learning.

C2k provides every pupil and member of staff with a unique username to access C2k services. Authenticated users are granted access to C2k's filtered internet service. User activity is logged and reports of usage are available to nominated staff, including the principal, within the college. For both staff and pupils, the use of the school's information technology resources is a privilege which can be removed. Where inappropriate use of the internet is suspected, the facility to remove access for a user may be applied and any subsequent access monitored.

Once available through C2k, the college will utilise 'Securus' , an eSafety monitoring system that helps teachers identify cyber-bullying and other child protection concerns. On detection of inappropriate words or phrases, an alert is sent to IT support staff to allow immediate intervention and action in line with the Acceptable Use Policy.

Risk Assessments

The Head of E-Learning will conduct a periodic risk assessment of the school technologies, recording any issues and reporting these to the Leadership Team in order to secure and enhance eSafety arrangements. Each social media technology that is to be utilised will be risk assessed in the context of curricular need and safety provision.

Each subject head will perform risk assessments on the materials and technologies within their curricular specification to ensure that they are fully aware of and can mitigate against the potential risks involved with their use.

Authorising internet access

The C2k Education Network internet filtering assesses all websites based on their content and access to the most inappropriate sites, including those on the Internet Watch Foundation banned list will always remain blocked. This applies across the C2k network, whether using a C2k core desktop computer or a personal iPad.

The system categorises all websites as either red (unavailable) or green (available). By default, all users are given access to a core set of green sites.

In addition to the default sites, the college can choose to make users members of one or more internet-related security groups. These are:

Internet Social Networking: This group provides access to Facebook, Twitter, LinkedIn, Wordpress.

Internet Streaming: This group provides access to YouTube, BBC iPlayer, Vimeo and other television and radio streaming sites.
Internet Advanced: This group provides access to sites in a range of categories. These include: Webmail, Shopping, Drugs and Alcohol, Sex Education

College staff will have access to these sites for the purpose of teaching and learning and student access will only be through sight of materials downloaded for teaching and under the supervision of a teacher.

Students in Applied Business Studies at A-Level have access to Internet Advanced to facilitate coursework requirements; students have been informed of the dangers and responsibilities associated with this access, the work is monitored by the Head of Business Studies and any breach of school policy is deemed to be serious as to warrant suspension/expulsion depending upon the nature of the offence. The Head of e-Learning may, at any point, request a review of the access made by such students from C2k.

The college can request that individual sites be arbitrated by C2k. The sites in question will be reviewed against a range of headings including: security, educational content, ethical and moral content. Sites may then be moved between Red and Green categories depending on the outcome of this process. Parents, staff or pupils who consider the content of a site to be inappropriate are encouraged to report this to the principal. Staff are aware that use may be monitored by the principal and designated staff.

Pupils coming across inappropriate material or situations online are encouraged to report these to their form tutor. Parents wishing to report inappropriate use of on-line materials within or outside school should contact the Head of Key Stage regarding pupils and the principal regarding staff.

All members of the school and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's processes. Reports are logged and the college will seek support from C2k and/or PSNI, as appropriate, in dealing with e-safety issues.

Mobile Technology

Pupils may be given access to mobile tablets and they will make use of the meru wireless technology provided by C2K through the C2K shared access username and password or C2KOpenguest. It is the responsibility of the classroom teacher to monitor and control the use of the tablets and to ensure that pupils engage in appropriate use.

Cyber Bullying

Pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. Where this form of bullying occurs in school, actions taken are those within the college's anti -bullying and behaviour policies to protect the victim and ensure that the bullying is ended. Where it is deemed appropriate or where cyber-bullying is reported as having taken place outside school, parents will be advised to contact the PSNI.
Cyber Bullying can take many different forms and guises including:

- Email – nasty or abusive emails which may include viruses or inappropriate content.
- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive

messages perhaps using a compromised or alias identity.

- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile.
- Online Gaming – abuse or harassment of someone using online multi-player gaming sites.
- Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.
- Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

Pupils are made aware through the pastoral programme and in school assemblies, posters and class discussion that cyber-bullying can constitute a criminal offence under the Protection from Harassment (NI) Order 1997, Malicious Communications (NI) Order 1988 and The Communications Act 2003 The college will keep a record of cyber-bullying incidents on file to monitor the effectiveness of their preventative activities, and to review and ensure consistency in any investigations, support and sanctions.

The college also provides guidance to parents (see below) via the college website to help deal with incidents of cyberbullying and inappropriate use of the internet.
General advice to everyone:
We all deserve to be able to use the internet to learn, explore and connect with each other. But all of us need to be aware of the risks involved in doing so, especially on social media. Our advice is:

- *Don't share personal information or images with people you don't know.*
- *Don't accept friend requests with someone you don't know – not everyone online may be who they say they are.*
- *Set privacy settings on all devices so that only people you know can view your account.*
- *Don't post anything online that you are not happy to be shared, particularly nude or nearly nude images or videos. It may seem like a bit of fun with friends at the time but there is always a chance those images could be shared or get into the wrong hands and could lead to harmful situations such as stalking, abuse or blackmail.*
- *If someone has made you feel uncomfortable or you have had disturbing interaction online, tell police or a trusted adult. You can ring the police on 101 or for help and advice ring Childline on 0800 1111 or Lifeline on 0808 808 8000.*
- *The internet can be a great place but it is important to remember there are people out there who may wish to abuse, exploit, intimidate or bully you online – if this happens to you, tell someone immediately.*
- *Remember that if things do go wrong online, there are people who can help.*
- *If you receive any inappropriate images or links, it is important that you do not forward it to anyone else. Contact police or tell a trusted adult immediately. By doing this you could help prevent further such incidents. You will not get into trouble.*

General advice to parents:

- *The most important thing is to have conversations with your children - talk to them about the benefits and dangers of the internet so that you can empower them to use the internet safely.*
- *Cultivate an interest in their online activities - their favourite websites, online games and interests and keep an eye on what they are doing online.*

- *Don't be afraid to ask your children who they are talking to online and what they are talking about and remind them how important it is to tell a trusted adult if something happens online that makes them feel uncomfortable or worried because there are people who can help.*
- *Become a 'net-savvy' parent - the best safeguard against online dangers is being informed. Jump in and learn the basics of the Internet - read articles, take a class, and talk to other parents. You don't have to be an expert to have a handle on your child's online world.*
- *Go to www.getsafeonline.org for lots of useful advice and information on how to stay safe online. Safeguardingni.org will also provide information for parents and carers on e-safety.*
- *Links to other sites that can provide information and advice to young people and parents are available from the DE website at: http://www.deni.gov.uk/index/pupils-and-parents/pupils.htm*

Email security

The C2k Education Network filtering solution provides security and protection to C2k email accounts. The filtering solution offers scanning of all school email ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content.

All staff and pupils are encouraged to use their C2k email system and staff should not use home email accounts for school business.

All users are expected to sign up to and adhere to the Acceptable Use Policy which is reviewed annually. This policy reminds all users of their responsibilities whenever they are using the Internet and includes accepted rules of ICT etiquette. Staff and pupils accessing the Internet via the C2k Education Network will be required to authenticate using their C2k username and password. This authentication will provide Internet filtering via the C2k Education Network solution. Access to the Internet via the C2k Education Network is fully auditable and reports are available to the school principal.

Social Media

All members of the Lumen Christi College community will be encouraged to engage, where appropriate, in social media in a positive, safe and responsible manner at all times. Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the school community.

Managing information systems

The school is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats.

For more information on data protection in school please refer to our Data Protection Policy.

Non C2k Networks

For the purpose of Child Protection and eSafety, pupils may not use mobile phones at any time during the school day and their use in photographing of other pupils is a serious breach of school rules and Child Protection requirements liable to suspension from school.

Reducing online risks

Lumen Christi College is aware that the Internet is a constantly changing environment. Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school computer or device.
The school will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.

Communication and review of the eSafety policy

The school eSafety policy will be updated biennially or when new technologies are introduced and after a risk assessment has been completed. Parents, pupils and staff have been consulted in the formulation of this policy and will be informed of any amendments made as required.

Engagement and education of staff

Teachers are the first line of defence in eSafety; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to illegal activity. Staff will participate in training and support to determine what action is appropriate including when to report an incident of concern to the school Designated Teacher for Child Protection or Mrs Matthewson, Head of e-Learning with responsibility for eSafety. eSafety training will thus be an element of staff induction and the on-going continuous professional development programme.

It is also important that staff understand their individual responsibilities in the use of internet, including social media, in terms of eSafety for themselves and others. Staff bringing their own device to school and using it for school purposes will thus be required to adhere to a number of key behaviours:

- Teachers bringing their own devices to school must ensure that access to the device is locked, that they have an individual, personal and strong password security shared with no other individual, use encryption where possible to store data securely and delete any data inputted or stored relating to pupils or staff once redundant.
- Staff should ensure that the choice of devices used are limited to those which have an appropriate level of security for the data being downloaded and register the device with a remote locate and wipe facility to maintain confidentiality of data in the event of a loss.
- Any photographs of pupils taken by school staff on other devices such as mobile phones, ipads, etc. will be submitted on to the school website or stored school facility and immediately deleted from the teacher's personal device. The personal usage of such devices will be for school

purposes only and staff will not retain images of pupils for any other purpose. Parental permission for pupils to be included in school photographs is obtained each year.

- Staff must not store any information relating to the school, staff or pupils on public cloud- based sharing or public backup services.
- Staff using school-owned technology outside school must at all times ensure that hardware, pen drives and software are locked securely away when not in use and that no student or staff data is maintained on devices beyond the time of use.
- References to colleagues, students, parents or school in e-mails used both in school and for school purposes may mean that the individual or institution referred to can ask to see what has been written. Even on personal devices and private accounts, inappropriate comments may give rise to complaints.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff in a variety of ways, on a regular (at least annual) basis.
- Members of staff with a responsibility for managing filtering systems or monitor ICT use will be supervised by the Leadership Team and will have clear procedures for reporting issues or concerns.

Engagement and education of parents and carers

A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, fetes and sports days.

Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.

Information and guidance for parents on online safety will be made available to parents in a variety of formats.

Parents will be encouraged to role model positive behaviour for their children online.

Responding to Online Incidents and Safeguarding Concerns

All members of the school community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.

All members of the school community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.

The Designated Teacher for Child Protection will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded. They will ensure that online safety concerns are escalated and reported to relevant agencies.

Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Education Authority and the PSNI if there is immediate danger or risk of harm.

If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Authority.

Communicating via the school website and Twitter

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects. The Vice Principal will approve the publication of information to the website; publishing and maintenance will be overseen by the Senior Teacher for e-learning.

Twitter will be used to communicate on a day-to-day basis about events within the College. The Senior Teacher with responsibility for PR assisted by the Senior Teacher for e-Learning will oversee the Twitter account.

Online Safety (e-Safety) References

National Links and Resources

Action Fraud: www.actionfraud.police.uk
BBC WebWise: www.bbc.co.uk/webwise
CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
ChildLine: www.childline.org.uk
Childnet: www.childnet.com
Get Safe Online: www.getsafeonline.org
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF): www.iwf.org.uk
Lucy Faithfull Foundation: www.lucyfaithfull.org
Know the Net: www.knowthenet.org.uk
Net Aware: www.net-aware.org.uk
NSPCC: www.nspcc.org.uk/onlinesafety
Parent Port: www.parentport.org.uk
Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/
Think U Know: www.thinkuknow.co.uk
Virtual Global Taskforce: www.virtualglobaltaskforce.com
UK Safer Internet Centre: www.saferinternet.org.uk
360 Safe Self-Review tool for schools: https://360safe.org.uk/
Online Compass (Self review tool for other settings): http://www.onlinecompass.org.uk/

References

www.deni.gov.uk
http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety
www.swgl.org.uk
www.eani.org.uk