LURGAN COLLEGE

ONLINE SAFETY POLICY

Introduction

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. Currently the internet technologies children and young people are using, both inside and outside of the classroom, include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst these ICT resources can be exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with the use of Internet technologies.

In Lurgan College we understand the responsibility to educate our pupils in Online Safety issues. We aim to teach them appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. Online Safety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. This main purpose of this policy is to help pupils keep themselves safe when using online technologies.

Online Safety in the school context:

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

Our school has a duty of care to enable pupils to use on-line systems safely. The rapidly changing nature of the Internet and new technologies means that Online Safety is an ever growing and changing area of interest and concern. This Online Safety policy reflects this by responding to current and emerging issues relating to online safety; this is done through annual review of the policy.

Dangers Relating to Pupils' Use of The Internet

The Internet is a unique and exciting resource. It brings the world into the classroom by giving children and young people access to a global network of educational resources. There is no doubt that the use of the Internet is an essential skill for young people as they grow up in the modern world. (Further detail can be found in Lurgan College's *Acceptable Use of ICT and the Internet Policy* - Subsection 1. Rationale for pupil use of ICT).

The Internet is, however, an open communications' channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials some of which could be unsuitable. Key Concerns are:

1. Potential Contact

Pupils may come into contact with someone on-line who may wish to harm them. Some adults use social networks, chat rooms or e-mail to communicate with young people for inappropriate reasons

Pupils will be reminded:

- That people are not always who they say they are.
- That they should never give out personal details.
- That they should never meet alone anyone contacted via the Internet.
- That once they publish information it can be disseminated with ease and cannot be destroyed. That others may disseminate personal or sensitive information to threaten, intimidate or coerce them to do something they would not otherwise do.

2. Inappropriate Content

Through the Internet there are unsuitable materials in many varieties. Anyone can post material on the Internet. Some material is published for an adult audience and is unsuitable for young people of school age e.g. materials with a sexual content.

Materials may express extreme views e.g. some use the web to publish information on weapons, crime and racism which would be restricted elsewhere. Materials may contain misleading and inaccurate information. e.g. some use the web to promote activities which are harmful such as anorexia or bulimia.

Pupils will be reminded:

- That information on the Internet is not always accurate or true.
- To question the source of information.
- How to respond to unsuitable materials or requests and that they should tell a teacher/adult immediately.

3. Conduct - Cyber Bullying

Staff should be aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. This form of bullying is considered within the school's overall anti-bullying policy and pastoral services as well as the Online Safety policy.
Care should be taken when making use of social media for teaching and learning - further guidance is given in Lurgan College's *Acceptable Use of ICT and the Internet Policy.*

Cyber Bullying can take many different forms and guises including:

- Messages or posts which are abusive, threatening or designed to damage the self-esteem of someone else. These messages or posts may include viruses or inappropriate content. They are often sent or published via email, Instant Messaging (IM), chat rooms, social networking sites, or online gaming. These message are often sent or posted using a compromised or alias identity.
- 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.

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils are reminded that cyber-bullying can constitute a criminal offence. While there is no specific legislation for cyber-bullying, the following may cover different elements of cyber-bullying behaviour:

- Protection from Harassment (NI) Order 1997 (http://www.legislation.gov.uk/nisi/1997/1180)
- Malicious Communications (NI) Order 1988 (http://www.legislation.gov.uk/nisi/1988/1849)
- The Communications Act 2003 (http://www.legislation.gov.uk/ukpga/2003/21)

It is important that pupils are encouraged to report incidents of cyber-bullying to parents/guardians, the school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases.

4. Excessive Commercialism

The Internet is a powerful vehicle for advertising. In visiting websites young people have easy access to advertising which is very persuasive.

Young people should be taught:

- Not to fill out forms with a lot of personal details.
- Not to use an adult's credit card number to order online products.

If young people are to use the Internet in places other than at school e.g. – libraries, clubs and at home, they need to be educated about how to behave on-line and to discuss problems. There are no totally effective solutions to problems of Internet safety and there is a responsibility on teachers, pupils and parents to be vigilant in order to protect young people when using the Internet.

Roles and Responsibilities

As Online Safety is an important aspect of strategic leadership within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the Senior Leader with responsibility for ICT, the ICT Co-ordinator and pastoral staff to keep abreast of current Online Safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The Senior Leader with responsibility for ICT has overall responsibility for leading and monitoring the implementation of Online Safety education and policy throughout the school. The Vice Prinicpal (Pastoral) who is also the designated teacher for child protection has overall responsibility for pastoral matters relating to Online Safety; she is supported in this role by the deputy designated teacher, the Head of Year and House Teacher of the pupil(s) involved in any Online Safety incident or complaint.

The Principal and Senior Leader with responsibility for ICT update the Senior Leadership Team and Governors with regard to Online Safety and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Writing and Reviewing the Online Safety Policy

This policy, supported by the school's Acceptable Use Agreements for staff and pupils, is to protect the interests and safety of the whole school community. It is linked to other school policies including the *Acceptable Use of ICT and the Internet*, *Bring Your Own Device*, *Promoting Positive Behaviour, Health and Safety*, *Child Protection*, and *Anti-bullying*.

It has been agreed by the Senior Management Team, Staff and approved by the Governing Body. The School Council have also discussed the policy and members' views have been taken into account when developing this policy. The Online Safety policy and its implementation will be reviewed annually.

Online Safety Skills Development for Staff

- All staff receive regular information and training on Online Safety issues through the ICT co-ordinator (or Senior Leader with responsibility for ICT) as part of Child Protection training and at MLT meetings and other staff training sessions as necessary.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff members receive information on the school's Acceptable Use Agreement as part of their induction.
- All staff are encouraged to incorporate Online Safety activities and awareness within their lessons.
- Staff are encouraged to use the C2k videoconferencing facility to ensure security and privacy are maintained for pupils. This ensures only invited participants are enabled to contribute to the videoconference.

All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource. All staff will be given a paper or electronic copy of the School's Online Safety Policy and its importance explained.

Online Safety Information for Parents/Carers

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website.
- The school will communicate relevant Online Safety information through newsletters, Parentmail communications, messages from the Lurgan College Twitter account and the school website.
- Parents are given advice on the use of ICT at home in Lurgan College's *Acceptable Use of ICT and the Internet Policy* (subsection 9).

Educating Pupils in Online Safety Strategies

The school will plan and provide opportunities within a range of curriculum areas to teach Online Safety. Online Safety is also systematically addressed through the Personal Development Programme and through special assemblies such as the *Safer Internet Day* assembly. Online Safety is discussed at liaison meetings between Lurgan College and our principal feeder school, Lurgan Junior High School and the programmes and strategies used in Lurgan College seek to build on the work done there.

- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Child line/CEOP.
- The school Internet access is filtered through the C2k managed service.
- No filtering service is 100% effective; therefore all pupil use of the Internet access provided by the school is supervised by an adult.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. This is done through pupil induction sessions, information in the student planner, lessons in the PD programme, special assemblies (such as the Safer Internet day assemblies) and via

presentations from visiting organisations. For example, the use of the Internet is a planned activity. Aimless surfing is not encouraged.

Pupils are made aware of the school's rules on acceptable and safe use of ICT through induction day sessions, student planners, induction sessions at the beginning of each school year and through the publicising of school policies. Pupils are not given permission to use the school's facilities without first signing a written agreement to abide by the school's policies relating to ICT.

Password Security:

- Pupils and staff users are provided with an individual login username and password, which they must change periodically. Login details should not be shared with anyone else. Under no circumstances should staff share with pupils the login details of any other member of staff.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network. For example, staff should never leave their computer or network-connected device unlocked and staff should exercise caution to ensure confidential or sensitive information is not displayed inadvertently on their interactive whiteboard.

Handling Online Safety Complaints and Concerns:

- Parents/guardians should notify the Vice Principal (Pastoral Care) of any school related activities involving the internet which cause concern.
- Complaints of Internet misuse will be dealt with by the Senior Leader with responsibility for ICT or the VP Pastoral depending on the nature of the complaint. Following any misuse of ICT or the Internet, sanctions will be imposed in accordance with the schools *Promoting Positive Behaviour Policy.*
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator and recorded in the Online Safety incident logbook.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

- **Related Documents / Circulars**
- Lurgan College – Policy for the Acceptable Use of ICT and the Internet
- Lurgan College - Bring Your Own Device Policy
- Lurgan College - Anti-Bullying Policy
- Lurgan College - Child Protection Policy
- Lurgan College - Promoting Positive Behaviour Policy
-
- DENI Circular 1999/25
- DENI Circular 2007/01
- DENI Circular 2011/22
- DENI Circular 2013/25
- DENI Circular 2015/21
- DENI Circular 2016/26
- DENI Circular 2016/27

Reviewed June 2017

BECTA guidance on responding to Online Safety incidents.