Larne High School

Policy statement
In relation to
e-Safety

October 2021

1.INTRODUCTION

1.1 Introduction

Larne High School identifies that the internet and associated devices, such as computers, tablets, mobile phones, and games consoles, are an important part of everyday life. These allow immediate access to email, searching for information on the internet, access to subject resources and other functions such as access to social networking sites e.g. Facebook, Instagram and blogging sites.

We recognise and value the increasingly wide opportunities that information technology provides to our staff and pupils. Whilst it is our aim that all members of our school community avail as fully as possible of this technology, we also appreciate the need for safeguards to be in place. Young people have many opportunities to benefit from the use of these devices, however their use needs to be carefully managed.

Larne High School believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

1.2 What is the Internet and Virtual Learning Environment (VLE)?

The Internet is an electronic information highway connecting many thousands of computers all over the world and millions of individual subscribers. This global "network of networks" is not governed by any entity. This means that there are no limits or checks on the kind of information that is maintained by, and accessible to, Internet users. The educational value of appropriate use of information and resources located on the Internet is substantial.
A Virtual Learning Environment (VLE) is a range of educational resources, comprising information, forums, quizzes and other online material provided to pupils as part of an online learning package.

1.3 Rationale for pupil use of the Internet and VLE

Larne High School encourages use by pupils of the rich information sources available on the Internet and VLE, together with the development of appropriate skills to analyse and evaluate such resources. On-line resources offer a broad range of up-to-date resources to pupils, provide an independent research facility, facilitate a variety of learning styles and abilities and encourage pupils to take responsibility for their own learning. Internet and VLE and e-mail literacy are fundamental requirements for all pupils as preparation for the Information Age – an era where ICT is a dominant factor in work and home life.

1.4 Links with other School Safeguarding Policies

The policy is linked to the school's Pastoral Care, Child Protection, Sustaining Positive Behaviour and Internet policies and the Pupil Code of Conduct.
The Anti-Bullying Policy seeks to create a safe and caring environment in which effective teaching and learning can take place and all pupils are given the opportunity to develop to their full potential.

2. THE AIMS OF THE POLICY

The policy aims to:

- Safeguard and protect all members of the Larne High School community online.
- Identify approaches to educate and raise awareness of e-Safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to e-Safety concerns.

Larne High School identifies that the issues classified within e-Safety are considerable, but can be broadly categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material.
- **Contact:** being subjected to harmful online interaction with other users.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

3. PROCEDURES

3.1 Cyberbullying

Bullying, intimidation and harassment are not new in society; however, bullying via electronic methods of communication both in and out of school represents a new challenge for schools to manage.

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 should be considered within the College's overall Anti- bullying Policy and pastoral services as well as the eSafety policy.

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be 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 both the school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases.

These guidelines are intended to help a school make explicit the expectations of the school on pupil use of mobile phones and the restrictions which are placed on their use in school and on school grounds. The guidelines sit alongside the Acceptable Use Policy which all pupils sign and is shared with parents and carers. They also give clear guidance to staff, pupils and parents about the consequences for breaches of the guidelines.

3.2 Youth Produced Sexual Imagery

The school recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the Designated Teacher for Child Protection. The school will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods. We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using school provided or personal equipment.

We will not:

• view any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so - If it is deemed necessary, the image will only be viewed by the Designated Teacher for Child Protection and their justification for viewing the image will be clearly documented.

• send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- act in accordance with our safeguarding and child protection policies.
- store the device securely.

3.3 Online Hate

Online hate content, directed towards or posted by, specific members of the community will not be tolerated at the school and will be responded to in line with existing policies, including Anti-bullying and Behaviour. All members of the community will be advised to report online hate in accordance with relevant policies and procedures.

The Police will be contacted if a criminal offence is suspected.

4. RESPONSIBILITIES

4.1 Board of Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy.

4.2 Principal & SLT

- The Principal has a duty of care for ensuring the safety (including online) of members of the school community.
- The Principal and Senior Leaders are responsible for ensuring that the relevant staff receive suitable training to enable them to carry out their e-safety roles.
- The member(s) of SLT with responsibility for e-learning, leads the E-Learning Group, takes responsibility for online safety responsibilities, takes a lead in reviewing policy, liaises with Head of ICT and technical support staff, receives reports of online safety incidents, maintains a log and reports regularly to the SLT.
- The Senior Leadership Team will ensure that there are appropriate and up-to-date policies regarding e-Safety; including a Behaviour Policy, which covers acceptable use of technology

4.3 C2K Managers & School Technicians

Those with technical responsibilities are responsible for ensuring:

- that the technical infrastructure is secure and is not open to misuse or malicious attack and meets required online safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Principal and Senior Leaders
- that monitoring systems are implemented and updated as agreed in school policies

4.4 Teaching and Support Staff

Are responsible for ensuring that:

- read and adhere to the e-Safety policy and acceptable use policies
- take responsibility for the security of school systems and the data they use or have access to
- model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site
- e-safety issues are embedded the curriculum and other activities where appropriate
- have an awareness of a range of e-Safety issues and how they may be experienced by the pupils in their care
- identify e-Safety concerns and take appropriate action by following the school's safeguarding policies and procedures
- know when and how to escalate e-Safety issues, including signposting to appropriate support, internally and externally
- pupils follow the e-Safety Policy
- instructing pupils regarding 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

4.5 Designated Child Protection Officer

Should be aware of the potential for serious child protection/safeguarding 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
- cyber-bullying

4.6 E-Learning Group

Members take the lead with regards to:

- the production/review/monitoring of the school e-safety policy
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/filtering/incident logs
- consulting stakeholders – including parents/carers and the students/pupils about the e-safety provision

4.7 Pupils:

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement
- should 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
- will be expected to know 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 and realise that the school's e-safety policy covers their actions out of school, if related to their membership of the school

4.8 Parents/carers

It is the responsibility of parents/carers to:

- read the acceptable use policies and encourage their children to adhere to them
- support the school's e-Safety approaches by discussing e-Safety issues with their children and reinforcing appropriate and safe online behaviours at home
- role model safe and appropriate use of technology and social media
- identify changes in behaviour that could indicate that their child is at risk of harm online
- seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online
- contribute to the development of the e-Safety policies
- use school systems, such as learning platforms, and other network resources, safely and appropriately
- take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies

5. LEARNING PLATFORM

5.1 Management of Learning Platforms

Larne High School uses Satchel One as its official learning platform. Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities. Only current members of staff (except Governing Body, Contractors and Visitors), pupils and parents will have access to the LP. When staff and pupils leave the setting, their account will be disabled. Pupils and staff will be advised about acceptable conduct and use when using the LP. All users will be mindful of copyright and will only upload appropriate content onto the LP.

Any concerns about content on the LP will be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive
- If the user does not comply, the material will be removed by the administrator
- Access to the LP for the user may be suspended
- The user will need to discuss the issues with a member of leadership before reinstatement
- A pupil's parents/carers may be informed
- If the content is illegal, we will respond in line with existing child protection procedures

Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame. A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

6. ACCEPTABLE USE OF DIGITAL IMAGES OF PUPILS

All staff should follow the guidance below when dealing with taking, display, storage and use of photographs and digital images of pupils.

6.1 Taking of Photographs/Video of Pupils

Parents will be asked to give their consent in writing to a range of such activities. A central database on the C2k system will be maintained of those pupils for whom parental permission has and has not been received. Staff will be required to consult this database prior to taking any images of pupils.

6.2 Display/use of Photographs/Video of Pupils

Staff are permitted to capture and/or use images of pupils for whom parental permission has been appropriately received, for display purposes and publicity in and outside school, in school publications, on the school digital signage and website. Where staff require additional guidance on the display/use of photographs the Principal should be consulted. The Principal must grant permission for images of pupils to be distributed to any external media provider.

6.3 Capture & Storage of Photographs/Video of Pupils

Staff should use the school camera kept in the office for the taking of photographs for school business. It is recognised, however, that in many circumstances, (for example field trips, sporting events or incidental activities within departments) this is not always possible or appropriate. In these circumstances, staff are encouraged to capture images of pupils using hardware which has been procured by the school. Furthermore, it should not be normal practice to store digital images of pupils (however obtained) on school or personal laptops or on any external memory device as a matter of course for prolonged periods of time. As a result staff should ensure that:

1. Any image/s of a pupil/s (from camera, scanner or other source) that is/will be stored digitally should be stored within the “Private 4” folder on the school C2k network. Technical support will be available from the ICT support staff to assist in the transfer of existing/new images.
2. Staff must transfer digital media from capture devices to the “Private 4” folder on the school C2k network at the earliest possible opportunity. In order to maximise the efficient use of school resources, staff should do this by ensuring that:

    a. ONLY files which are most suitable for school business are selected
    b. selected files are copied to Private 4>School Photo>Year e.g. “2021”
    c. remaining images from the camera or initial capture device are deleted
    d. images are located in an appropriately named folder. (Consider Activity - Form – Month – Staff Code to be appropriate e.g. “History Trip February CW”)

3. Staff should not pass images of pupils to third parties without consulting the Principal.
4. Staff are discouraged from storing images of pupils on laptops, however, it is recognised that, to facilitate editing or selection this may be essential. In these circumstances, personal laptops should not be used. It is expected that, after initial use by staff, digital images of pupils should be deleted from laptops or external memory devices as soon as possible.
5. Traditional photographs of pupils should continue to be stored within departments using scrapbooks or a suitable alternative.
6. Any member of staff requiring further advice should consult the Principal.
7. Some subjects, for example Physical Education, have specialist course requirements which necessitate the use of digital images of pupils to address essential course criteria. In some circumstances, technical limitations of the C2k system prevent files from being usefully stored within the staff resources area. In subjects where these circumstances have been identified, the storage of digital images is permissible on external storage devices providing:

1. the device is owned by Larne High School and

2. the device is normally retained within the school building.

There may be a need, at intervals throughout the year, to facilitate formative and summative feedback or assessment. In these circumstances, the device may be taken home by the staff member concerned providing:

1. all reasonable precautions are taken to ensure the security of the device and

2. the device is returned to school at the earliest opportunity.

7. INFORMATION MANAGEMENT

The school values the importance of appropriate data management procedures and practices and requires all staff to be prudent regarding sensitive personal materials, whether paper based or electronic.
Staff are encouraged to use SIMS.net to access the personal information of pupils. Access to SIMS.net is only provided within school and is always password encrypted.

Staff must not store electronic copies of sensitive personal information on

1. any personally or school owned device e.g. personal memory sticks, laptops , tablet devices or desktop computers (sensitive personal information should only be saved to staff members' "My Documents" rather than to the hard drive of the device) nor
2. portable storage devices e.g. portable hard-drive or memory stick. (Neither School procured nor personally owned portable devices are considered acceptable for sensitive data)

Staff may store basic pupil information electronically, for example, name, tutor group, report comment and performance statistics, for the purposes of recording pupil achievement throughout the year. This information may be removed from the school building to facilitate assessment activities including report-writing. Staff are advised that any document, saved on a portable storage device, containing information about pupils should be password protected. Staff are also asked to be prudent about the sensitivity of this data and are asked to maintain its confidentiality, for example the data should not be accessed in a public place.

Since the transformation of the C2k network in July 2014, all staff have access to both their "My Documents" and school Private Folders through the internet via the C2k "cloud" servers. While C2k is responsible for ensuring appropriate and secure encryption of all data accessible on their servers, staff are responsible for ensuring that they close the browser window and properly log off after accessing this facility so that information cannot be viewed by anyone else who may have access to a shared device; they ensure that information is not accessed in a public place.

8.SOCIAL MEDIA

8.1 Expectations

The expectations regarding safe and responsible use of social media applies to all members of the Larne High School community. The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger. All members of the Larne High School community are expected to engage in social media in a positive, safe and responsible manner.

All members of the Larne High School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others. We will control pupil and staff access to social media whilst using school provided devices and systems on site.

Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.

8.2 Staff Personal Use of Social Media

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities. Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policies. All members of staff are advised to safeguard themselves and their privacy when using social media sites.

Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Setting the privacy levels of their personal sites
- Being aware of location sharing services
- Opting out of public listings on social networking sites
- Logging out of accounts after use
- Keeping passwords safe and confidential
- Ensuring staff do not represent their personal views as that of the school

8.3 Pupils' Personal Use of Social Media

Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age-appropriate sites and resources. Any concerns regarding a pupil's use of social media will be dealt with in accordance with existing policies, including anti-bullying, behaviour and safeguarding. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games, or tools.

Pupils will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present
- To use safe passwords
- To use social media sites which are appropriate for their age and abilities

- How to block and report unwanted communications
- How to report concerns both within the setting and externally

8.4 Official Use of Social Media

Larne High School does have a couple of official social media accounts. The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes. Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.

Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only. Official social media sites are suitably protected and, where possible, run and linked to our website. Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.

Official social media use will be conducted in line with existing policies, including: Anti-bullying, Data Protection, Safeguarding and Child Protection. All communication on official social media platforms will be clear, transparent and open to scrutiny.

Parents/carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community. Written parental consent will be obtained, as required. Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used. Any official social media activity involving pupils will be moderated.

9. ACCEPTABLE USE OF ELECTRONIC DEVICES

9.1 Pupils' Use of Personal Devices and Mobile Phones

Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

Larne High School expects pupils' personal devices and mobile phones to be kept in a secure place and kept out of sight during lessons. Mobile phones or personal devices will not be used by pupils during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff. The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.

Mobile phones and personal devices must not be taken into examinations. Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

If a pupil breaches the policy, sanctions and interventions will be applied in relation to Pupil Choice and Consequence found in the Appendix of the Sustaining Positive Behaviour Policy. Staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene our behaviour or anti-bullying policy or could contain youth produced sexual imagery (sexting). The following would apply:

- Searches of mobile phone or personal devices will only be carried out in accordance with our Behaviour, Child Protection and Safeguarding Policies
- Pupil's mobile phones or devices may be searched by a member of the Senior Leadership Team, with the consent of the pupil or a parent/carer. Content may be deleted or requested to be deleted, if it contravenes our Behaviour, Child Protection and Safeguarding Policies
- Mobile phones and devices that have been confiscated will be released to parents/carers
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation

9.2 Examples of acceptable and unacceptable use

On-line activities which are encouraged include, for example:

- the use of email and computer conferencing for communication between colleagues, between pupil(s) and teacher(s), between pupil(s) and pupil(s), between schools and industry;
- use of the Internet and VLE to investigate and research school subjects, cross-curricular themes and topics related to social and personal development;
- use of the Internet and VLE to investigate careers and Further and Higher education;
- the development of pupils' competence in ICT skills and their general research skills.

On-line activities which are not permitted include, for example:

- searching, viewing and/or retrieving materials that are not related to the aims of the curriculum or future careers;
- searching, viewing and/or retrieving offensive materials (this includes sexually explicit material or material of a sexual nature);
- copying, saving and/or redistributing copyright protected material, without approval;
- subscribing to any services or ordering any goods or services, unless specifically approved by the school;

- playing computer games or using other interactive ‘chat’ sites, unless specifically assigned by the teacher;
- using the network in such a way that use of the network by other users is disrupted (for example: downloading large files during peak usage times; sending mass email messages);
- publishing, sharing or distributing any personal information about a user (such as: home address, email address, phone number, etc.);
- sending or receiving unsavoury, insensitive, offensive or obscene e-mails;
- any activity that violates a school rule;
- using any equipment to photograph, record or video any school activity or person for which or from whom explicit permission has not been given;
- using or distributing, including on social networking sites, any material relating to school activities, pupils or staff for which explicit permission has not been given; this includes the posting of material, images or video footage relating to Larne High School staff, pupils, the school environment or school name without prior written consent from the Principal or his appointed deputy. This applies to curricular and extra-curricular aspects of school life as well as to all school trips; engaging in any activity that is harmful of or hurtful to others.

10. ADVICE TO PARENTS

10.1 Introduction

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Larne High School will take every opportunity to help parents understand these issues. 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/Learning Platform and on-line student/pupil records

● their children's personal devices in the school

10.2 Additional Advice for Parents with Internet Access at Home

1. The computer with Internet access should be situated in a location where parents can monitor access to Internet. Computers should be fitted with suitable anti-virus, anti-spyware and filtering software. Access to the internet through mobile technologies makes supervising your child's online activity much more difficult. It is important to discuss with your child the dangers of the internet and to ensure that internet filtering settings are activated on all mobile devices.

2. Parents should discuss with their children the school rules for using the Internet and implement these at home. Parents and children should decide together when, how long, and what comprises appropriate use.

3. Parents should get to know the sites their children visit and talk to them about what they are learning.

4. Parents should consider using appropriate Internet filtering software for blocking access to unsavoury materials. Further information is available below.

5. It is not recommended that any child under 16 should be given unmonitored access to newsgroups or chat facilities.

6. Parents should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school's name, or financial information such as credit card or bank details. In this way they can protect their children (and themselves) from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud.

7. Parents should encourage their children not to respond to any unwelcome, unpleasant, or abusive messages, and to tell them if they receive any such messages or images. If the message comes from an Internet service connection provided by the school or by C2k, they should immediately inform the school.

8. Please note for your own information that many social networking sites have a minimum age restriction. In the case of Facebook, for example, the recommended age for use of this site is 13 years of age.

Further free advice for parents is available from the following sources:
http://www.thinkuknow.co.uk/ - a website designed to inform children of the potential hazards involved with online chatrooms.
http://www.parentsonline.gov.uk/ - promotes home school links by helping parents understand the role of Information Communications Technology (ICT) in learning. www.kidsmart.org.uk
http://www.wiseuptothenet.co.uk/ - The Home Office guide to Internet safety with downloadable leaflets for parents
http://www.getnetwise.org/ - information about filtering programs for home use

11. USE OF PERSONAL DEVICES AND MOBILE PHONES

11.1 Expectations

Larne High School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within the school.

All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as Anti- bullying, Behaviour and Child Protection and Safeguarding.

Electronic devices of any kind that are brought onto site are the responsibility of the user.

All members of the Larne High School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.

All members of the Larne High School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.

All members of the Larne High School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our Behaviour, Safeguarding or Child protection Policies.

12. REVIEW & EVALUATION

12.1 This Policy will be reviewed and updated as appropriate and on a regular basis and in the light of changing legislation, developments in technology or best practice guidance by the Senior Leadership Team in consultation with the school Pastoral team and pupils.

Policy Review Date: August 2024

Appendix 1

Cyber Safety Advice

Pupils are not permitted to access social networking sites via the school network. However, the following guidelines are suggested to ensure pupil safety and security when using these websites outside school.

- Do not give out or post personal information online – report it to a trusted adult and/or use this website https://www.thinkuknow.co.uk/
- Make sure that social networking account privacy settings are set at "friends only" or "protected".
- Do not accept friend requests from anyone you do not know in person.
- Do not post private details such as home address, mobile or home telephone numbers or other personal details.
- Never post photographs that have been taken in your bedroom
- Never post photographs of others without their permission.
- Never give out your mobile number.
- If you get messages or images which upset you, do not reply. Keep a record and report them to a trusted adult or your network provider.
- Think before you send messages or images – once you send them you cannot control them. Never pass on rude or embarrassing images or messages.
- Sexting of images is illegal for both sender and receiver.
- If someone makes you feel uncomfortable online – report it to a trusted, responsible adult and/or use the thinkuknow.co.uk website
- Respect other people's privacy as well as your own.
- Do not make someone else uncomfortable online.
- Do not use a social networking site to bully another pupil including the editing and posting of inappropriate images, messages or comments or any aspects of cyberbullying.
- Be aware of the legal consequences of your online activities.

You are not anonymous online. All deleted material can be retrieved, and correspondence can be sourced through the computer's IP address.

REMEMBER You can be traced online or on your mobile phone

Be careful about what you say, what you upload, what you send, what you store.

Appendix 2

STAFF EQUIPMENT LOAN AGREEMENT

Staff must comply with the following conditions.

- All School resources (including computers, cameras, laptops, tablet devices) and their associated accessories are provided for educational use; they must not be used for any other purposes. Only portable resources (such as laptops, ipads, tablet devices) may be removed from school, to facilitate preparation for teaching and learning, in accordance with the details set out below. Additionally, the resources may not be passed on to any third party.
- All electronic devices are expensive and therefore must be looked after appropriately and must be kept in a safe place, including those taken off site.
- All staff are reminded that it is the responsibility of individual staff taking electronic devices off-site to provide adequate insurance cover for the full-replacement cost of the electronic device including software and accessories. This amount can be advised by the E-Learning Coordinator or the Bursar.
- No equipment or resources can be taken off-site without the prior permission of the person in charge of those resources.
- Users must not give unauthorised access to any confidential material relating to the School or its pupils.
- It is the duty of the user to ensure that all electronic devices are protected by a passcode and/or password and passwords and access codes are kept strictly confidential.
- Use of all ICT equipment (including tablet devices) must be in line with the School's ICT Acceptable Use, eSafety and Digital Media Policy. This applies not only when the equipment is being used in school, but also when it is being used off-site. School-owned ICT equipment (including tablet computers) is to be used only by current members of staff of Larne High School.
- Equipment is loaned to members of staff only for the duration of their employment in Larne High School. All equipment must be returned when a member of staff ends their period of employment in the School. Staff off school for an extended period of time (e.g. due to longterm illness, maternity leave, career break) will be expected to return any school-owned equipment in their possession so it can be utilised by someone else.

  Staff wishing to take any electronic device off-site must have signed below to indicate their agreement of these conditions, a copy of which will be retained by the Principal.

  I have read and understood the School's ICT Acceptable Use, eSafety and Digital Media Policy and agree to abide by this policy.

  I accept responsibility for the full replacement value of all equipment which I take off-site.

  I accept that before taking any equipment out of School I must have the permission of the teacher in charge of those resources.

  Name: _____ (Please Print)

  Signed: _____

  Date: _____

Appendix 3

Internet Filtering within School

1. Access to the internet using the C2k System

The C2k service provides Larne High School with the necessary hardware, software and connectivity to enable access to the internet. Access is controlled, by C2k, through a filtering mechanism. A filtering service, no matter how thorough, can never be comprehensive, and it is essential that all staff and pupils have a clear understanding of the Acceptable Use Policy, and that adequate supervision is maintained.

Despite the filtering process, it is possible for unsuitable websites to become available, sometimes for short periods after they are launched. If at any time school pupils find themselves able to access, from within the school, internet sites which they think should be blocked, they should advise their teacher immediately. Likewise staff should immediately advise the member of the Senior Leadership Team with responsibility for ICT (or, in his/her absence, another member of the Senior Leadership Team) giving details of the site address and the time and date of access.

To resolve the situation and enable C2k to maintain an effective filtering mechanism, the member of the Senior Leadership Team with responsibility for ICT should contact C2k by emailing filtering@c2kni.net or by telephoning the C2k Helpdesk at 0870 6011666 with details of the site(s).