Updated August 2020

Movilla High School

eSafety Policy

Providing for success…..

Raising attainment …..

October 2019

Ratified by
Board of Governors
October 2019

Updated August 2019

Movilla High School eSafety Policy

August 2015 - Amended 2020

Policies relating to the Use of ICT:

Acceptable Use Policy

Health and Safety relating to ICT

Codes of Conduct

eSafety Policy

ICT Department Policy

Contents

Introduction

This eSafety Policy forms part of the Safeguarding Guidance of Movilla High School and supplements the Code of conduct for staff, visitors and students, the Home School Partnership agreement, Pastoral Care suite of policies and Acceptable Use Policy. We consider the welfare of everyone in our educational community to be of the utmost importance and this policy promotes the welfare of our students as set out in Articles 17 & 18 of the Education and Libraries (Northern Ireland) Order 2003.

The Internet and associated technologies is seen as an essential tool to support teaching and learning, as well as playing an important role in the whole school community. The main ICT facility in Movilla High School is the C2K Education Network.

This policy provides advice and guidance about eSafety and identifies the risks involved in using the Internet and associated technologies. Whilst total elimination of all risks is not achievable, Movilla High School outlines the steps it is taking to avoid/minimise these risks. The main objective is to develop a set of safe and responsible behaviours by the whole school community that will enable avoidance/reduction of the risks whilst continuing to enjoy the many benefits and opportunities offered by the Internet. Our expectations for responsible and appropriate conduct are formalised in the Acceptable Use Policy (AUP) that all staff and students must follow at all times.

As part of its commitment to eSafety, Movilla High School recognises its obligation to implement a range of security measures to protect the school network and ICT facilities from attack, compromise or inappropriate use and to protect school data.

This eSafety policy should be read in conjunction with the Pastoral Care suite of policies of Movilla High School listed below:

- Safeguarding and Child Protection Policy
- Information and Communications Technology Policy
- Acceptable Use Policy
- Anti-Bullying Policy
- Home School Partnership Agreement
- Mobile Phone Policy

It has also taken account of the following Department of Education Circulars:

1. Circular on Acceptable Use of Internet and Digital Technologies in Schools Number 2007/1
2. Circular on Internet Safety Number 2011/22
3. Circular on eSafety Guidance Number 2013/25
4. Empowering Schools Strategy (March 2004)
5. Safeguarding and Child Protection in Schools – A Guide for Schools (June 2016)

At Movilla High School, we believe it is crucial for everyone to be aware of the offline consequences that online behaviour can have. Breaches of this eSafety policy will be taken very seriously and may lead to civil, disciplinary and/or criminal action being taken against parties involved.

What is eSafety?

eSafety is short for electronic safety; it is a term which not only refers to the internet but to other ways in which people communicate using electronic media, e.g. mobile phones, gaming devices and wireless technology. It means ensuring students, their parents and staff are protected and supported to achieve the maximum benefit from new and developing technologies without risk to themselves or others.

The aim of promoting eSafety is to protect young people from the adverse consequences of using electronic media, including bullying, inappropriate sexualised behaviour or exploitation. It includes educating the whole educational community of Movilla High School on risks and responsibilities and forms part of the 'duty of care' which applies to everyone working with children.

The world of ICT is a fast moving environment and covers a wide range of resources including: mobile learning, web-based learning and Virtual Learning Environments (VLE) to name but a few. Some of the technologies available to young people in/outside of school are:

- Mobile/Smartphones features include; video, pictures, texts and web access
- Blogs & Wikis based on Web 2.0 technologies
- Online Forums, Chat Rooms, Social Networking i.e. Facebook, Instagram, Snapchat, Twitter, etc.
- Music and Video Broadcasting
- Laptops, Tablets, PDAs, PCs, Voting Systems
- Websites e.g. You Tube
- Podcasting
- Email & Instant Messaging –e.g. MSN, Outlook
- Virtual Learning Environment –e.g. Fronter

The school's Acceptable Use and ICT Policies cover both fixed and mobile technologies within school (such as PCs, Laptops, PDAs, Tablets, Webcams, Smartphones, Voting Systems etc.)

Helping its students to stay safe online will always be a priority for Movilla High School. As technology changes so new risks emerge. As a school, we will continue to work hard with our partner agencies to keep up with such a rapidly moving scene.

This policy is designed to provide guidance and support to students, parents and staff of the risks they face online and particularly to ensure the most vulnerable are protected from harm.
This strategy is a revised version of the 2013 version and will be reviewed annually by the eSafety team and Senior Leadership team prior to endorsement by the Board of Governors.

eSafety is very important and it is the responsibility of the eSafety team and Board of Governors to ensure that the eSafety policy is implemented. It is also the eSafety team's duty to ensure that through careful planning and actions an eSafety programme is developed and forms an integral part of the school curriculum.

For clarity, the lead person for eSafety within Movilla High School is called the eSafety Coordinator and is supported by an eSafety Team.

The eSafety team comprises:

Principal	Mr I Bell
eSafety co-ordinator	Miss B McCord (also ICT Manager)
Designated Teacher	Mr I Bell
Designated Governor for Child Protection	Mr S Doherty

Policy approved by the Board of Governors _____
Date _____
Date for next policy review _____

ROLES AND RESPONSIBILITIES

eSafety is the responsibility of the whole school community and everyone has their part to play in ensuring that they are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities highlight how each member of the school community will contribute.

eSafety Team Responsibilities:

- Develop and promote an eSafety culture within the school community and take ultimate responsibility for the eSafety of the whole school community.
- Appoint an eSafety co-ordinator to take responsibility for eSafety throughout the school and support the eSafety team.
- Provide clear channels of communication for the eSafety coordinator to liaise with the whole school community
- Liaise with the school's Board of Governors by having eSafety regularly on the agenda of Board meetings.
- Ensure that access to the school's ICT system is as safe and secure as reasonably possible.
- Ensure that servers and other key hardware or infrastructure are located securely with appropriate staff permitted access.
- Ensure adequate technical support is in place to maintain a secure ICT system.
- Ensure that a comprehensive eSafety education programme with appropriate resources is in place and delivered to all staff, students and parents.
- Ensure that the school's Child Protection Officer(s) receive training to address the challenges presented by the use of the Internet and new technologies.
- Ensure policies and procedures are in place to ensure the integrity of the school's information and data and that procedures are in place to prevent personal data being sent over the Internet unless such data is encrypted or made secure.
- Ensure that all users are informed that school equipment must not be used to view and transmit inappropriate material. (The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer".)
- Ensure that all staff and students agree to the Acceptable Use Policy (AUP) and that new staff have eSafety included as part of their induction procedures.
- Receive and regularly review eSafety incident logs; ensure that the correct procedures are followed should an eSafety incident occur in school and review incidents to see if further action is required.
- Ensure that parents/guardians are offered opportunities to increase their knowledge of how ICT is used by their children and the eSafety issues arising from that use
- Ensure that only technical staff/C2K administrators are permitted to download and install software onto the C2K network.
- Ensure that all users of the C2K Education Network have been made members of the appropriate internet group.
- Manage the C2k service Internet categories of web sites that are available to users and recommend to the Board of Governors any sites they wish to be assessed for blocking or unblocking by completing the C2k Filtering Request Form (cf Information Sheet No EN039 Managing Internet Filtering)

eSafety Co-ordinator Responsibilities

- Promote an awareness and commitment to eSafety throughout the school.
- Be the first point of contact in school on all eSafety matters.
- Create and maintain eSafety policies and procedures working with members of the eSafety. team and other staff members as appropriate.
- Develop an understanding of current eSafety issues, guidance and appropriate legislation.
- Ensure delivery to all staff and students of an appropriate level of training in the full range of eSafety issues identified in this policy.
- Ensure that an eSafety education programme is in place and embedded across the curriculum.
- Ensure that staff and students know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable.
- Liaise with school technical staff and C2k for the blocking of inappropriate websites, social network sites and other unsuitable digital material.
- Ensure that eSafety is promoted with parents/guardians and advice given as to how they can. support their children should they become victims through the Internet and other technological malpractice.
- Ensure that all staff and students understand the contents of the Acceptable Use Policy and that it is signed, returned and filed securely.
- Ensure that any person who is not a member of school staff, who makes use of the school ICT equipment in any context, is made aware of the Acceptable Use Policy.
- Ensure that all members of the school community understand the consequences of not following the regulations set in the Acceptable Use Policy which they have signed.
- Monitor, report and advise on eSafety issues to the eSafety team, Senior Leadership Team and Governors as appropriate.
- Advise the eSafety Team of your future training needs to fulfil your role of eSafety Co-ordinator.
- Liaise with the Local Educational Authority and other relevant agencies as appropriate.
- Ensure an eSafety incident log is kept up-to-date.
- Ensure that Good Practice Guides for eSafety are displayed in classrooms and around the school.

Responsibilities of all Staff

- Read, understand and help promote the school's eSafety policies and guidance.
- Read, understand and adhere to the Staff AUP.
- Develop and maintain an awareness of current eSafety issues and legislation and guidance relevant to their work.
- Maintain a professional level of conduct in their personal use of technology at all times.
- Take responsibility for ensuring the safety of sensitive school data and information.
- Be responsible for, or assist with the delivery of the eSafety education programme to students, ensuring that students fully understand the requirements of the Student AUP and that it is duly signed.
- Supervise students carefully when engaged in learning activities involving technology.
- Ensure that students are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable.
- Foster a culture that students feel able to report any cyber-bullying, 'grooming' abuse or receipt of inappropriate electronic materials.
- Be aware of how to advise students who receive uninvited/unwelcome attention or are presented with inappropriate materials as a result of their use of the new technologies.
- Inform and periodically remind students that their use of the Internet is monitored.
- Remind students not to share their password with any other person.
- Encourage students to keep back-ups of all their work and to name their USB memory pens so that ownership can be established in the event of loss.
- Preview all websites which they intend to incorporate into their teaching or use only sites accessed from managed 'safe' environments such as the school VLE.
- Be vigilant when students are researching with search engines such as Google.
- Respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- Report all eSafety incidents which occur to the principal, C2K manager, or designated teacher.
- Report any failure of the filtering systems to the C2K manager.

Responsibilities of Students

- Read, understand and adhere to the Student AUP and follow all guidance about safe practice.
- Take responsibility for their own and each others' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school.
- Remember not to share their password with any other person.
- Reminded to name their USB memory pen so that ownership can be established in the event of loss.
- Remember to take back-up copies of any files which they generate.
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening.
- Report all eSafety incidents to appropriate members of staff.
- Discuss eSafety issues with family and friends in an open and honest way.

Responsibilities of Parents and Guardians

- Help and support the school in promoting eSafety.
- Read, understand and promote the Student AUP with their children.
- Discuss eSafety concerns with their children, show an interest in how they are using. technology, and encourage them to behave safely and responsibly when using technology.
- Be aware of those sites which can offer advice and support to children who receive uninvited/ unwelcome attention or are presented with inappropriate materials as a result of their use of the new technologies.
- Consult with the school if they have any concerns about their child's use of technology.
- Avail of any training / information sessions on eSafety offered by Movilla High School.

Responsibilities of Technical Staff

- Ensure that servers, workstations and other hardware and software are kept updated as appropriate.
- Ensure that a firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date.
- Check that staff have virus protection installed on all laptops/tablets used for school activity.
- Maintain the C2K filtered broadband connectivity.
- Liaise with C2k and take steps to immediately remove access to any website considered inappropriate by staff or students
- Ensure that only approved or checked webcam sites are available for staff /student use
- Keep up-to-date with C2k services and policies
- Ensure appropriate technical steps are in place to safeguard the security of the school ICT system, sensitive data and information. Review these regularly to ensure they are up to date
- At the request of the Senior Leadership Team conduct occasional checks on files, folders, email and other digital content to ensure that the Acceptable Use Policy is being followed
- Report any eSafety-related issues that come to their attention to the eSafety coordinator and/or eSafety team/Senior Leadership Team
- Ensure that procedures are in place for new users and leavers to be correctly added to and removed from all relevant electronic systems
- Ensure that suitable access arrangements are in place for any external users of the school's ICT equipment
- Ensure that any administrator or master passwords for school ICT systems are kept secure and available to at least two members of staff, e.g. Principal and C2K Manager.
- Ensure that the wireless network is protected by a secure login which prevents unauthorised access.
- Liaise with C2K and others on eSafety issues.

Responsibility of any external users of the school systems e.g. adult or community education groups

- Take responsibility for liaising with the school on appropriate use of the school's ICT equipment and Internet.
- Ensure that participants are trained in the requirements set out in the Temporary Staff/Visitors AUP and that this policy has been signed by the participants.

Responsibilities of Governing Body

- Ensure that there is an up-to-date eSafety policy in place.
- Read, understand, contribute to and promote the school's eSafety policies and guidance as part of the schools overarching safeguarding procedures.
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafety awareness.
- Ensure appropriate funding and resources are available for the school to implement their eSafety strategy.

Learning and Teaching

Developing safe and responsible behaviours online within the school community of Movilla High Schoool, lies in an effective eSafety programme. The Internet and other technologies are part of our students' lives, inside and outside school. Education in appropriate, effective and safe use of the Internet is an essential element of the school curriculum. This education is as important for staff and parents as it is for students. Educating students on the dangers of technologies that may be encountered outside school is done as part of eSafety in partnership with associated external agencies including Community Safety Forum, PSNI, visiting theatre/drama groups and informally when opportunities arise. Movilla High School will:-

- Develop an environment that encourages students to tell a teacher/responsible adult immediately if they encounter any material that makes them feel uncomfortable.
- Ensure students and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or eSafety co-ordinator.
- Ensure students and staff know what to do if there is a cyber-bullying incident.
- Ensure all students know how to report abuse.
- Have a clear, dynamic eSafety education programme throughout all Key Stages. Teach students a range of skills and behaviours appropriate to their age and experience, such as:
    - be vigilant online at all times
    - develop a range of strategies to validate and verify information before accepting its accuracy, e.g. is it fact, fiction or opinion
    - quickly skim and scan information
    - develop analytical skills to recognise bias
    - use search engines that are more effective in getting results and how to narrow down searches
    - develop good "Netiquette".
- understand how photographs can be manipulated:
    - understand why on-line 'friends' may not be who they say they are and to understand importance of being careful in online environments
    - understand why they should never post or share details about themselves, their personal lives, any contact information, details about their daily routines, photographs and videos and to know how to ensure they have turned-on privacy settings
    - understand why they must never post pictures or videos of others without their permission
    - understand why and how some people will 'groom' people for sexual reasons

  - understand legislation when working online, particularly copyright of music files etc.
  - understand why care should be taken in downloading software in case of viruses
  - have strategies for dealing with receipt of inappropriate content or email.

- Ensure that when copying materials from the web, staff and students understand issues around plagiarism, how to check copyright and also know that they must observe and respect copyright/ intellectual property rights.
- Ensure that staff and students understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups, buying on-line, on-line gaming/ gambling.
- Ensure staff know how to encrypt data where confidentiality is required and that they understand data protection and general ICT security issues linked to their role and responsibilities.
- Provide training to staff on eSafety.

Internet Access

Web filtering of internet content is provided by C2K. This ensures that all reasonable precautions are taken to prevent access to inappropriate material. However, it is not possible to guarantee that access to unsuitable material will never occur. Teachers are encouraged to preview websites they wish to use in advance. All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer. Notices are posted in classrooms and around school as a reminder.

The school decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary login.

All users are provided with a login appropriate to their key stage or role in school. Students are taught about safe practice in the use of their login and passwords. All users should only be using the Internet for a legitimate need.

Staff are given appropriate guidance on managing access to laptops/tablets which are used both at home and school and in creating secure passwords.

Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information.

Remote access to the C2K school system is covered by specific agreements and is never granted to unauthorised users.

Using the Internet

The school provides the internet to:

- Support curriculum development in all subjects;
- Facilitate and encourage independent learning and research by students;
- Support the work of staff as an essential professional tool;
- Enhance the school's management information and administration systems;
- Enable electronic communication and the exchange of curriculum and administration data with the Department of Education, the Examination Boards, Education Authority and others.

Users are made aware that they must take responsibility for their use of, and their professional conduct whilst using, the school ICT systems or a school-provided laptop or device and that such activity can be monitored and checked.

All users of the school ICT or electronic equipment will abide by the relevant Acceptable Use Policy (AUP) at all times, whether working in a supervised activity or working independently,

Students and staff are informed about the actions to take if inappropriate material is discovered and this is supported by notices in classrooms and around school.

Using email

Email is regarded as an essential means of communication and all members of the school community are provided with a C2K e-mail account for school-related communication. Communication by email between staff, students and parents will only be made using the school email account and should be professional and related to school matters only. E-mail messages about school business should be regarded in the same manner as communicating on headed notepaper and reflect a suitable tone and language to ensure that the good name of the school is maintained.

- All staff and students in school are given their own unique email address for school business only, this gives the ability to audit emails in a secure manner.

- It is the responsibility of each email account holder to keep their password secure. For the safety of all users email communications are filtered by C2k email filtering and logged and reports are completed on a regular basis.

- Staff should not contact students or parents or conduct any school business using a personal email address.

- Students should only use email for educational purposes under supervision from a teacher.

- Any abuse of the email system/policy witnessed by staff or students should be reported to the ICT Manager.

C2k operates an appropriate educational filtered Internet-based email system for schools.

Within the school context email should not be considered private and the school reserves the right to monitor e-mail. There is a balance to be achieved between monitoring to maintain the safety of students and the preservation of human rights, both of which are covered by recent legislation.

As part of the curriculum students are taught about safe and appropriate use of email. Students are informed that misuse of email will result in a loss of privileges.

All users are reminded that sending threatening e-mails and other messages is a criminal offence under the Protection from Harassment Act (1997), the Malicious Communications Act (1988) and Section 43 of the telecommunications Act (1984).

Using images, Video and Sound

It is recognised that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Students are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants; images and video are of appropriate activities and are only taken of students wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

All parents/carers are asked to sign an agreement about taking and publishing digital images and video of their children and this list is checked whenever an activity is being photographed or filmed.

For their own protection staff or other visitors to school never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of students.

The Acceptable use consent form is considered a valid document for the entire duration of the students' education at Movilla High School.

CCTV / WEBCAMS

Movilla High School has a CCTV infrastructure for the safety and security of all persons on the site. The only people that have access to CCTV real-time viewing are SLT and the system's maintenance team.

Any CCTV footage that is captured for security purposes is only available for viewing by the Principal, Vice Principal, SLT and the PSNI.

Webcams are used in school solely as a learning resource within ICT lessons or for staff training by outside agencies.

Staff may use web cams for online learning through Google Meet.

Using Video Conferencing and other Online Meetings

Video conferencing is used to enhance the curriculum by providing learning and teaching activities that allow students to communicate with people in other locations. Staff and students take part in these opportunities in a safe and responsible manner. All video conferencing activity is supervised by a suitable member of staff. Students do not operate video conferencing equipment, answer calls or set up meetings without permission from a member of staff.

All participants are made aware if a video conference is to be recorded. Permission is sought if the material is to be published.

For their own protection a video conference or other online meeting between a member of staff and pupil(s) which takes place outside school or whilst the member of staff is alone is always conducted with the prior knowledge of the principal or a member of SLT and respective parents/carers.

Publishing Content Online (a) School Website:

The school maintains editorial responsibility for any school-initiated web site or virtual learning platform content, to ensure that content is accurate and the quality of presentation is maintained. The school maintains the integrity of the school web site by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the web site is the school address, e-mail and telephone number. Contact with staff is through the receptionists in the school office.

Identities of students are protected at all times. Photographs of individual students are only published on the web with parental permission and group photographs do not have individual pupils identified. The school obtains permission from parents for the use of students' images.

VLE, Blogs, Wikis, Podcasts, Social Network Sites

As part of the curriculum students are encouraged to create online content. Students are taught safe and responsible behaviour in their creation and publishing of online content. They are taught to publish for a range of audiences which might include governors, parents or younger children. Blogging, podcasting and other publishing of online content by students will take place within the school virtual learning platform or other media selected by the school. Students will only be allowed to post or create content on sites where members of the public have access, when this is part of a school related activity. Appropriate procedures to protect the identity of students will be followed.

All reasonable steps are taken to ensure that any material published online is the author's own work, gives credit to any other work included and does not break copyright.

Online Material Published outside the School:

Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school.

Material published by pupils, governors and staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.

SOCIAL MEDIA SAFEGUARDS

Facebook and Twitter Safeguards

The school does have a Facebook account.

- Staff are reminded of their personal and online safety when they access, update or post profiles of themselves (Safeguarding and Child Protection Policy; Staff Code of Conduct refers). Violations of their personal security or online safety should be notified immediately to the Principal or the ICT Manager. The Designated Teacher will also be informed where issues of Child Protection are raised.
- The school will defend its reputation and that of its stakeholders against any unacceptable online activity which includes:
  (a) Breaches of the Acceptable Use of ICT Policy
  (b) Breaches of Safeguarding and Child Protection Policy
  (c) Defamation of students or staff of the school
  (d) Harassment or cyberbullying of any pupil or member of staff
  (e) Breaches of Data Protection Policy (disclosure of personal information)
  (f) Posting of derogatory or offensive remarks about the school, its staff or students
  (g) Posting photographs obtained from any school publication or website which have been digitally altered to convey an unacceptable image of the individual or the school.

MOBILE TECHNOLOGIES

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as PDAs, portable media players, gaming devices, mobile and smart phones are familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus can open up risk and misuse associated with communication and internet use. All emerging technologies that the school intends to use will be thoroughly examined and tested by the eSafety team before implementation in the classroom. The management of the use of devices so that users exploit them appropriately is as follows:

- The school allows staff to bring in personal mobile phones and devices for their **own** use. **Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device.** Staff are not permitted to use their mobiles during class teaching time (Safeguarding and Child Protection Policy; Staff Code of Conduct refers). Exception: There are occasions when the ICT Manager or technician may have to use their mobile phones to talk with C2K staff to solve problem with pupil's computer or digital files.

- The school's Mobile Phone and Safeguarding and Child Protection policies outline how pupil and staff use of mobiles is managed. If a pupil is found using a mobile device for personal reasons on the school premises the device will be confiscated, sent to the office for secure storage before being issued back to the pupil at the end of the school day. Students who have breached the Mobile Phone Policy on three occasions, will have their phone returned only to a parent.

- The sending of inappropriate text, image and video messages between any member of the school community, inside or outside school is not allowed. External agencies will be involved if a criminal offence is suspected. The Designated teacher will also be involved if Child Protection concerns are raised.

- Under no circumstance must content created on the mobile device be uploaded to any web site that shares information i.e. Facebook, Instagram, Snapchat or YouTube that contains any member of the school community whether in school or at home. The only exceptions are to the school's Virtual Learning Network (VLN) Google Classroom, school website, school's Facebook and the player in the reception area, with permission. External agencies will be involved if a criminal offence is suspected. The Designated teacher will also be involved if Child Protection concerns are raised.

SAFE USE AND STORAGE OF IMAGES

All staff shall follow the guidance below when dealing with taking, display storage and use of photographs and digital images of pupils. This is in line with the Safeguarding and Child Protection Policy.

It shall **not be** normal practice to store digital images of pupils (however obtained) on school or personal laptops as a matter of course for **prolonged** periods of time. As a result staff shall ensure that:

1 Any image/s of a pupil/s (from camera, scanner or other source) that is/will be stored digitally shall be stored on central storage area. Technical support will be available from the ICT Manager to assist in the transfer of existing/new images to central area.
2 Photographs of pupils shall not be stored in the Pupil Shared Documents. If photographs have to be stored they shall be stored in the Staff Shared area.
3 Archived photographs will be stored on CD-ROMs or a centralised storage area for long term storage.

USE OF SECURUS SOFTWARE TO MONITOR USE OF C2K DEVICES

Securus is a safeguarding tool to monitor online and application use. This tool was introduced to Movilla High School in August 2017 and will be used to monitor activity using the following technologies:

- Key stroke monitoring
- Application monitoring
- Optical character recognition.

The software alerts the school to anything that suggests that a student may be at risk or in breach of AUP. Issues and concerns that can be detected by Securus are:

- Cyberbullying
- Online grooming and child abuse/exploitation
- Depression, self-harm and suicide
- Racial, homophobic and religious harassment
- Use of drugs or weapons
- Radicalisation and extremism

Pupils, staff and parents will be made aware of the purpose of the tool. Incidents reported by Securus will be investigated by ICT Manager or Principal and action taken will be in line with the eSafety policy.

MISUSE AND INFRINGEMENTS

Complaints relating to eSafety should be made to the ICT Manager (eSafety co-ordinator) or the Principal. The Designated Teacher will also be involved where Child Protection concerns are raised. All incidents will be logged.

HANDLING ESAFETY INCIDENTS

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be reported immediately to the eSafety co-ordinator and action in line with the eSafety policy will be taken.

- Deliberate access to or creation of inappropriate material by any user will lead to the incident being logged by the ICT Manager; investigation by the Principal, Vice Principal, ICT Manager and

/or Designated Teacher; immediate suspension possibly leading to expulsion and involvement of PSNI as deemed necessary by the investigation team.

- Any staff misuse that suggests a crime has been committed, a child has been harmed or that a member of staff is unsuitable to work with children will be reported to the Designated Teacher, Principal and Education Authority (South Eastern Region) CPSSS within one working day in accordance with EA (SER) Policy.

- Any complainant about staff misuse must be referred to the Principal and if the misuse is by the Prinicpal it must be referred to the Chair of Board of Governors in line with the EA (SER) Policy and the school's Safeguarding and Child Protection Policy.

- Students, parents and staff will be informed of the complaints procedure.

All eSafety incidents are recorded in the School eSafety Log which is regularly reviewed.

- Any incidents where pupils do not follow the Acceptable Use Policy will be dealt with following the school's normal disciplinary procedures.
- In situations where a member of staff is made aware of a serious eSafety incident, concerning pupils or staff, they will inform the eSafety coordinator or principal who will then respond in the most appropriate manner.
- Instances of cyberbullying will be taken very seriously by the school and dealt with using the school's anti-bullying procedures. School recognises that staff as well as pupils may be victims and will take appropriate action in either situation.
- Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's e-Safety coordinator and technical support and appropriate advice sought and action taken to minimise the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy, then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that pupil data has been lost.
- The school reserves the right to monitor school equipment used off-site and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.
- If an incident occurs which raises concerns about Child Protection or the discovery of indecent images on a computer, then the incident will be referred to the Designated Teacher and the Principal. The Child Protection Procedures of the school will be followed.

Activities consistent with unacceptable (possibly illegal) conduct

- accessing inappropriate or illegal content deliberately
- deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- continuing to send or post material regarded as harassment, or of a bullying nature after being warned
- using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)

Activities likely to result in disciplinary action:

- any online activity by a member of the school community which is likely to adversely impact on the reputation of the school
- accessing inappropriate or illegal content accidentally and failing to report this inappropriate use of personal technologies (e.g. mobile phones) at school or in lessons
- sharing files which are not legitimately obtained e.g. music files from a file sharing site
- using school or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the school into disrepute
- attempting to circumvent school filtering, monitoring or other security systems circulation of commercial, advertising or 'chain' emails or messages
- revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission
- using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content)
- transferring sensitive data insecurely or infringing the conditions of the GDPR May 2018.
- accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time
- accessing non-educational websites (e.g. gaming or shopping websites) during lesson time
- sharing a username and password with others or allowing another person to login using your account
- accessing school ICT systems with someone else's username and password
- deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else.

EQUAL OPPORTUNITIES

Students with additional needs

The school endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the school's eSafety rules.

However, staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety.

PARENT INVOLVEMENT

- Those with parental responsibility are asked to read through and sign any Acceptable Use Agreements on behalf of the child on admission to school and any annual Internet/Email agreement forms.

- Those with parental responsibility are required to make a decision as to whether they consent to images of their child being taken/used in the public domain i.e. school website.

- The school disseminates information to parents relating to eSafety where appropriate in the form of Information and celebration events, posters, Website/Learning Platform postings, Newsletter updates and VLE training.

REVIEWING THIS POLICY

This policy will be reviewed annually unless the school sees fit to add a change for security/safety reasons.

There will be an on-going opportunity for staff to discuss with the ICT Manager and or eSafety team, any issue regarding eSafety that concerns them.

The policy will be amended if new technologies are adopted , Local or National Government change the orders or guidance in any way and if DE Circulars require such change.

eSAFETY CONTACTS AND REFERENCES

CEOP (Child Exploitation and Online Protection Centre)	www.ceop.police.uk
Childline	www.childline.org.uk
Childnet	www.childnet.com
Click Clever Click Safe Campaign	http://clickcleverclicksafe.direct.gov.uk
Cybermentors	www.cybermentors.org.uk
Digizen	www.digizen.org.uk
Internet Watch Foundation (IWF)	www.iwf.org.uk
Kidsmart	www.kidsmart.org.uk
Think U Know website	www.thinkuknow.co.uk

Education Authority (South East Region) Child Protection Support Service for Schools
Grahamsbridge Road, Dundonald , Belfast, BT16 2HS

Mr Colum Boal	028 90 566434
Ms Alison Casey	028 90 566274

PSNI 0845 600 8000

eSafety RESOURCES

1. **Thinkuknow for Parents**
   https://www.thinkuknow.co.uk/parents
2. **A Parent'sguide to eSafety**
   http://whoishostingthis.com/resources/eSafety/
3. **BBC Bitesize safety**
   http://www.bbc.co.uk/bitesize/ks3/ict/history_impact_ict/esafety/activity/
4. **Parents' Guide to Technology – Safer Internet Centre**
   www.saferinternet.org.uk/advice-and-resources/parents-and-carers
5. **Parents and Carers- Childnet**
   www.childnte.com/parents-and-carers
6. **Online safety – Stop child abuse – support for children**
   www.nspcc.org.uk/help-and-advice/for-parents/onlineSafety/
7. **BBC WebWise – Top 10 online safety tips**
   www.bbc.co.uk/webwise/0/21259413
8. **Internet Safety for Parents and Children**
   www.parentsonlinesafety.com
9. **Internet Safety –Tips for parents about Internet safety**
   www.internetsafety.com/internet-safety-tips-for-parents.php
10. **Parents & Guardians – Child Exploitation and Online Protection**
    www.ceop.police.uk/safety-centre/Parents
11. **Online and mobile safety / Explore / ChildLine**
    www.childline.org.uk/explore/onlinesafety/pages/onlinesafety.aspx
12. **Online Safety / Safety Net Kids**
    www.safetynetkids.org.uk/personal-safety/onlineSafe

APPENDIX – PROCEDURE FOR A SEXTING INCIDENT

Definition of 'sexting'

For the purposes of this advice sexting is simply defined as:

'Sending or posting of sexually suggestive images, including nude or semi-nude photographs, via mobiles or over the internet.' (Safeguarding and Child Protection Policy page 12).

Pupils need to be aware that it is illegal, under the Sexual Offences (NI) Order 2008, to take, possess or share indecent images of anyone under 18. Additionally if a pupil is affected by inappropriate images or links on the internet, they need to be made aware that they **do not forward the image or link to anyone else.**

These images are shared between young people and/or adults via a mobile phone, handheld device or website with people they may not even know.

We recognise there are many different types of sexting and it is likely that no two cases will be the same. We realise the importance of carefully considering each case on its own merit and applying a consistent approach to help protect pupils, staff and the school.

1. What to do if a child makes a disclosure about a sexting, or suspected sexting incident: Whatever the nature of the incident, ensure school safeguarding and child protection policies and practices are adhered to. (Safeguarding and Child Protection Policy)
   - Act Promptly
   - Do not investigate yourself
   - Contact the designated teacher
   - Report your concerns and make full notes.

2. Searching the device

   Devices should not be searched unless the pupil is in immediate danger. Otherwise schools should follow the guidance from the DfE. Section 15 of 'Screening searching and confiscation – Advice for head teachers, staff and governing bodies' (2012) provides statutory guidance on searching electronic devices.

3. If indecent images of a child are found staff should:

   - Report the incident to the Designated Child Protection Teacher (following the child protection procedures set out in the school's Safeguarding and Child Protection policy).
   - The Designated teacher should assess the risk to the child or young person and make referrals as appropriate, taking advice from the Child Protection Team at EA if necessary.

   If the image has been shared on the school network, social network or website the school should:

   - Block the network to all users and isolate the image.
   - Images should not be moved, sent or printed.

4. Deciding on a response

    - It is important to remember that it won't always be appropriate to inform the police; this will depend on the nature of the incident. However, as a school it is important that incidents are consistently recorded. It may also be necessary to assist the young person in removing the image from a website or elsewhere.
    - Act in accordance with your child protection and safeguarding policy, e.g. notify Safeguarding team (Principal, Designated teacher, AVP for eLearning).
    - Store the device securely
    - Carry out a risk assessment in relation to the young person (Use Annex 1 and 2 of the report 'Sexting' in schools: advice and support around self-generated images)
    - Make contact with parents to inform them of the issues (where appropriate)
    - Make a referral if needed
    - Contact the police (if appropriate)
    - Put the necessary safeguards in place for the student, e.g. they may need counselling support, immediate protection and parents must also be informed.

5. Contacting other agencies If the nature of the incident is high-risk, we will contact PSNI.

    - Depending on the nature of the incident and the response you may also consider contacting your local police or referring the incident to CEOP.

6. Care provided after the incident

    The school will support the emotional and social well-being of the child / children who have been involved through:

    - Monitor and support their return to school
    - Refer to outside agencies where appropriate e.g. Barnardo's 'Safer Choices Programme'.
    - Offering access to a counselling service (where appropriate)