****

**S. Michael’s College, Enniskillen**

**E-Safety Policy 2018**

This policy is informed by DE guidance:

DE Circular 2007/01 Use of Internet and Digital Technologies in Schools

DE Circular 2011/22 Internet Safety

DE Circular 2013/25 e-Safety Guidance

DE Guidance on e-Safety June 2015

**Introduction**

St. Michael’s College has a duty of care to enable pupils to use on-line systems safely. E-Safety (electronic safety) is the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. The eSafety Policy refers not only to Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. Since ICT is a compulsory cross-curricular element of the revised curriculum, eSafety learning is built into the delivery of the curriculum itself. eSafety in the school context is concerned with safeguarding children and young people in the digital world; while it emphasises learning to understand and use new technologies in a positive way, it also focuses on education about the risks as well as the benefits so that users feel confident online and is concerned with supporting pupils to develop safer online behaviours both in and out of school and helping them recognise unsafe situations and how to respond to risks appropriately.

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

The policy should be read in conjunction with other school policies including Positive Behaviour Management, Child Protection/Safeguarding, Pastoral Care, Anti-Bullying and ICT Acceptable Use Policy (AUP).

**Digital Technologies**

**E-safety**

This policy, supported by the school’s acceptable use agreements for staff, governors and pupils is to protect the interests and safety of the whole school community. It is linked to the child protection policy and the school’s code of conduct.

ICT and on-line resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the staff on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote e-safety.

* Staff will receive information relating to e-safety.
* New staff will receive information on the school’s acceptable use policy as part of their induction.
* All staff will be made aware of individual responsibilities relating to the safe-guarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
* Pupils/parents/carers will be informed of where to seek advice or help if they experience problems when using the internet and related technologies, i.e. parent/carer, teacher, assistant, or an organisation such as Childline or CEOP.
* E-safety posters will be prominently displayed throughout the school.
* All users will be aware of the procedures for reporting accidental access to inappropriate materials i.e. the breach must be immediately reported to a C2K Manager.
* Deliberate access to inappropriate materials may lead to, depending on the seriousness of the offence:
* Being investigated by the Principal/C2K
* Possible immediate suspension
* Possibly leading to dismissal and involvement of PSNI for very serious offences.

**E-mail**

The use of e-mail within school is an essential means of communication for staff and students.

* By using your own school e-mail account you are clearly identified as the originator of a message.
* It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients all mail is filtered and logged. If necessary, e-mail histories can be traced.
* The use of or any other Internet web mail service for school business is not permitted.
* Under no circumstances should staff contact pupils, parents or conduct any school business using personal (non C2K) e-mail addresses.
* E-mails created or received as part of school business will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.
* Staff must immediately inform a C2K Manager if they receive an offensive e-mail.
* However you access your C2K e-mail (whether directly, through web mail when away from school or on non-school hardware) all the school e-safety policies apply.

**Internet Access**

All internet activity in St. Michael’s College is monitored and logged by our school service provider C2K. School work-stations can also be monitored by the school Principal and the C2K Manager. In order to maximise safe internet access:

* Staff will pre view sites before use.
* Care should be taken regarding image searches when working with pupils.
* All users must adhere to copyright in relation to software and online resources.
* Staff and pupils are aware that school based e-mail and internet activity can be monitored and explored further if required.
* If staff discover an unsuitable site the screen should be switched off/closed and the incident reported immediately to a C2K Manager.
* All staff and students must comply with the school’s ‘ICT Acceptable Use Policy’.

**Social Media Sites**

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

* Access to social media sites using C2K computers is forbidden unless you have been given permission by the Principal to access them and been given the appropriate C2k access rights.
* Access to social media sites using personal mobile phones during school hours is not permitted.
* Staff should not discuss any school related business on social media sites.
* Images of staff are not to be uploaded on to social media sites without the permission of the staff member/s involved.
* Staff must not accept pupils in the school and should exercise caution when accepting their parents as “friends” on social media sites; to do so leaves staff vulnerable to allegations of inappropriate contact and conduct and “friend” settings on Social Media do not guarantee privacy.

**Password Security**

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network:

* Staff should use their own personal passwords to access computer-based services.
* Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
* Staff should change temporary passwords at first logon and also change passwords whenever there is any indication of possible system or password compromise.
* Only disclose your personal password to a C2K Manager when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
* Staff should always lock their computer if they have to leave it unattended so that no-one else can access it.

**Roles and Responsibilities**

**Students:**

* Are responsible for using the school ICT systems in accordance with the ICT Acceptable Use Policy, which they must sign before being given access to school systems.
* Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
* Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
* Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school’s e-Safety Policy covers their actions out of school, if related to their membership of the school.

**Parents / Carers**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents’ evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

* Endorsing (by signature) the Student Acceptable Use Policy
* Accessing the school website in accordance with the relevant school Acceptable Use Policy.
* Parents/carers are expected to sign a Home School agreement (Data Capture Form - Appendix 3) which will contain the following statement:

*‘We will support the school approach to online safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community’*

Parents wishing to report inappropriate use of on-line materials within or outside school should contact the Form Teacher regarding pupils and the Principal regarding staff. The college will seek the support of C2k and/or PSNI, as appropriate, in dealing with e-safety issues. Advice may also be sought from the CPSSS (Child Protection Support Services in School) in relation to any Child Protection Concern.

The college also provides guidance to parents (Appendix 1) via the college website to help deal with incidents of cyber-bullying and inappropriate use of the internet.

**Curriculum Provision/Educating students**

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in safety is therefore an essential part of the school’s e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

* E-safety should be covered when appropriate in lessons e.g. use of social media, research, setting up accounts etc.
* Key e-safety messages should be reinforced as part of assemblies and tutorial /pastoral activities
* Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
* Students should be helped to understand the need for the student / pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
* Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
* Staff should act as good role models in their use of ICT, the internet and mobile devices.

Pupils are prepared within the curriculum to learn to recognise and avoid risks such as exploitation on the internet — to become “Internet-wise” and ultimately good “digital citizens”. The taught ICT programme provides direct eSafety learning at KS3 and eSafety/Cyberbullying is also a topic within the Personal Development pastoral programme***.***

**Staff**

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

* Staff should always log out after finishing work on-line; not logging out can mean the next user can access your social media account.
* Staff must not use school-owned equipment for personal social media purposes within or outside school; any such use is regarded as a serious breach of Acceptable Use.
* Staff should be aware that social media platforms can never be considered as private and all comments should be considered as “published” in terms of their language and content; while a lack of intent to publish may help in mitigation should the school take disciplinary action, comments may bring the school into disrepute or undermine a staff member’s role in the workplace.
* References to colleagues, students, parents or school in e-mails used both in school and for school purposes may mean that the individual or institution referred to can ask to see what has been written. Even on personal devices and private accounts, inappropriate comments may give rise to complaints.
* Staff using school-owned technology outside school must at all times ensure that hardware, pen drives and software are locked securely away when not in use and that no student or staff data is maintained on devices beyond the time of use.
* Teachers bringing their own devices to school must ensure that access to the device is locked, that they have an individual, personal and strong password security shared with no other individual, use encryption where possible to store data securely and delete any data inputted or stored relating to pupils or staff once redundant.
* Staff should ensure that the choice of devices used are limited to those which have an appropriate level of security for the data being downloaded. It is recommended that any access to school data when out of school is done through ‘Myschool’.

**Safe Use of Images**

**Taking, publication and storage of images**

Digital images are easy to capture, reproduce and publish and therefore, issue. We must remember that it is not always appropriate to take or store images of any member of the school community or public without first seeking consent and considering the appropriateness.

* The school permits the appropriate taking of images by staff with school equipment only with the written consent of parents/carers and staff.
* Where possible all recorded images and videos of pupils should be taken using the school camera, iPad or school mobile phone.
* Any photographs of pupils taken by school staff on other devices such as mobile phones, i-pads, etc will be submitted on to the school website or stored school facility and immediately deleted from the teacher’s personal device. The personal usage of such devices will be for school purposes only and staff will not retain images of pupils for any other purpose.
* If any member of staff does not want their photo to be used in any school publication or on the school website they must inform the Principal of this in writing.
* On a pupil’s entry to the school all parents/carers will be asked to give permission (Appendix 3) to use their child’s work/photos in the following ways:
	+ On the school website (or social media site)
	+ In the school prospectus and other printed publications that the school may produce for promotional purposes
	+ Recorded/transmitted on a video or webcam
	+ In display material that may be used in the school’s communal areas
	+ In display material that may be used in external areas e.g. exhibitions promoting the school
	+ General media appearances, e.g. local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically)
	+ For training purposes by related professionals
	+ This consent form is considered valid for the entire period that the pupil attends St. Michael’s College unless there is a change in the child’s circumstances where consent could be an issue e.g. divorce or parents/carers custody or child protection issues, etc.
	+ Teachers must check that permission has been given for their pupils’ images to be taken or published before an event takes place and before adding images to the website.
	+ Images of children are only permitted to be stored on the school’s C2K network or on authorised password protected external storage devices provided by the school.
	+ Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks).

**Cyber Bullying**

Pupils maybe subject to cyber bullying via electronic methods of communication both in and out of school. Where this form of bullying occurs in school, actions taken are those within the college’s anti -bullying and behaviour management policies to protect the victim and ensure that the bullying is ended. Where it is deemed appropriate or where cyber-bullying is reported as having taken place outside school, parents will be advised to contact the PSNI.

Cyber Bullying can take many different forms and guises including:

* Email – nasty or abusive emails which may include viruses or inappropriate content.
* Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
* Social media Sites – typically includes the posting or publication of nasty or upsetting comments on another user’s profile.
* Online Gaming – abuse or harassment of someone using online multi-player gaming sites.
* Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.
* Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person’s permission.

Pupils coming across inappropriate material or situations online are encouraged to report these to their form/ class teacher.

**Breaches**

A breach or suspected breach of policy by a school employee or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual. Any policy breach by staff is grounds for disciplinary action in accordance with the School Disciplinary Procedures, and the Education Authority procedures. Policy breaches may also lead to criminal or civil proceedings.

**Incident Reporting**

Any security breaches or attempts and any unauthorised use or suspected misuse of ICT must be immediately reported. Additionally, all lost or stolen equipment or data, virus notifications, unsolicited e-mails, misuse or unauthorised use of ICT and all other policy non-compliance must be immediately reported to the School Principal or a C2K Manager.

**Review Procedure**

* There will be an on-going opportunity for staff to discuss any issue of e-safety that concerns them.
* This policy will be reviewed every 24 months (or sooner in relation to advances in ICT, DENI guidance or if breaches have been detected). Consideration will be given to the implications for future whole school development planning.

|  |
| --- |
| **Appendix 1 (available on the school website)**General advice to everyone: We all deserve to be able to use the internet to learn, explore and connect with each other. But all of us need to be aware of the risks involved in doing so, especially on social media. Our advice is: * + Don’t share personal information or images with people you don’t know.
	+ Don’t accept friend requests with someone you don’t know – not everyone online may be who they say they are.
	+ Set privacy settings on all devices so that only people you know can view your account.
	+ Don’t post anything online that you are not happy to be shared, particularly nude or nearly nude images or videos. It may seem like a bit of fun with friends at the time but there is always a chance those images could be shared or get into the wrong hands and could lead to harmful situations such as stalking, abuse or blackmail.
	+ If someone has made you feel uncomfortable or you have had disturbing interaction online, tell police or a trusted adult. You can ring the police on 101 or for help and advice ring Childline on 0800 1111 or Lifeline on 0808 808 8000.
	+ The internet can be a great place but it is important to remember there are people out there who may wish to abuse, exploit, intimidate or bully you online – if this happens to you, tell someone immediately.
	+ Remember that if things do go wrong online, there are people who can help.
	+ If you receive any inappropriate images or links, it is important that you do not forward it to anyone else. Contact police or tell a trusted adult immediately. By doing this you could help prevent further such incidents. You will not get into trouble.

**General advice to parents:** * + The most important thing is to have conversations with your children - talk to them about the benefits and dangers of the internet so that you can empower them to use the internet safely.
	+ Cultivate an interest in their online activities - their favourite websites, online games and interests and keep an eye on what they are doing online.
	+ Don't be afraid to ask your children who they are talking to online and what they are talking about and remind them how important it is to tell a trusted adult if something happens online that makes them feel uncomfortable or worried because there are people who can help.
	+ Become a ‘net-savvy’ parent - the best safeguard against online dangers is being informed. Jump in and learn the basics of the Internet - read articles, take a class, and talk to other parents. You don’t have to be an expert to have a handle on your child’s online world.
 |

Source (DENI Pupil Support Team)

**Appendix 2**

**Acceptable Use Agreement/E-Safety Rules (Staff and Governors)**

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff and Governors are aware of their professional responsibilities when using any form of ICT. All staff are expected to read the school ICT Acceptable Use Policy, sign this policy and adhere at all times to its contents.

* I will only use the school’s e-mail/internet/and any related technologies for professional purposes or for uses deemed ‘reasonable’ by the Principal.
* I will comply with the ICT system security and not disclose any passwords provided to me by the school or C2K.
* I will ensure that all electronic communications with staff are compatible with my professional role.
* I will not give out my own personal details such as mobile phone number and personal e-mail address to pupils.
* I have been advised not to give out my own personal details such as mobile phone number and personal e-mail address to parents/carers.
* I will only use the approved, secure C2K e-mail system for any school business.
* I will ensure that school personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. All personal or sensitive data taken off-site must be kept secure.
* I will not install any hardware or software without the permission of a C2K Manager.
* I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
* Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or staff member.
* I will support the school approach to online safety and not deliberately share or upload any images, video or text that could upset or offend any member of the school community.
* I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Principal.
* I will respect copyright and intellectual property rights.
* I will ensure that my online activity, both in school and outside school, will not bring St. Michael’s College or my professional role into disrepute.
* I will support and promote the school’s e-safety and Acceptable use policies and help pupils to be safe and responsible in their use of ICT and related technologies in the context of school.
* I understand the sanctions related to breaches of the above.

**User Signature**

I have read the school Policy for E-safety and Acceptable Use of the Internet and Digital Technologies and agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Full Name (Printed) **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Signature **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_