MOUNT KELLY
Boarding and Day School
Boys and Girls, Aged 4-18

E-Safety Policy

(This policy applies to all staff and pupils including those in the EYFS)

Reviewed	January 2026
Next Review	January 2027
Owner	Deputy Head (Operations) / IT Department

Date of Review	Author	Page / Para	Synopsis of Amendment
16.01.2026	AS		Change of owner and combining separate policies into one E-Safety Policy
	AS		Including AI policy as written by Assistant Head – Teaching & Learning
	AS	Section 8 on pg 12	Added guidance for specific mobile phone usage in another section.
	AS		Added full acceptable usage to Appendix 1
	AS		Adapted name of IT manager throughout.
	AS		Added the introduction of Yondr locking pouches on pg 18

Contents

1. Online Safety Policy

I. School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

II. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

Relationships and sex education

Searching, screening and confiscation

UKCIS Safeguarding Children and Protecting Professionals in Early Years Settings

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

III. Roles and responsibilities

The governing body

The governing body has overall responsibility for monitoring this policy and holding the Head Master to account for its implementation.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety issues as provided by the designated safeguarding lead (DSL). This will take place via the safeguarding committee.

Review this policy annually and in response to any online-safety incident ensure that the policy is up to date, covers all aspects of technology use within the school, ensure online-safety incidents are appropriately dealt with and ensure that the policy is effective in managing such incidents.

The Head Master

The Head Master is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead (DSL)

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Head Master in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head Master, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged on MyConcern and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head Master and/or governing body

This list is not intended to be exhaustive.

The ICT Systems manager

The ICT Systems manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting security checks and monitoring the school's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that the DSL is made aware of any online safety incidents

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

In addition, EYFS staff will:

- supervise children whenever they are using devices
- Check apps, websites and tools prior to using them with children, including checking the results of searches
- Only use age-appropriate apps, websites and online tools
- Model safe practice when using technology
- Ensure data is shared online in accordance with the settings data protection responsibilities (From UKCIS Safeguarding Children and Protecting Professionals in Early Years Settings)

EYFS staff will also implement the required polices with regard to the safe use of mobile phones and cameras (see Safeguarding and child protection policy)

Parents

Parents are expected to:

- Support the School in its delivery of online safety by talking with their child / children about online safety issues and by reporting any incidents or concerns to the DSL as soon as they arise.
- Parents can also seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head Master and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Head Master.

Visitors and members of the community

- Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

IV. Educating pupils about online safety

- Pupils will be taught about online safety as part of the PSHE curriculum:

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

What Pupils will be taught

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private

Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of Year 6 school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- Understand what cyber-bullying is and what to do if they become aware of it happening to them or others
- Understand that sharing and viewing indecent images of children (including those created by children) is a criminal offence and carries severe penalties including jail
- Critically assess the trustworthiness of online content and identify different propaganda techniques and possible hidden agendas
- Understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- Recognise that malware is used to commit online crime and understand how to respond to social engineering techniques such as phishing
- Understand the impact social media can have on mental health, including body image, and how to identify strategies for dealing with online stress

Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online

- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- What 'grooming' is, how it can take place through the use of video games or social media, and how to report concerns about someone who makes contact online
- About the potential risks of online gambling and gaming, impact on mental and physical health and how to identify when behaviour has become problematic
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content including extremism, radicalisation, racism and misogyny and what to do and where to get support to report material or manage issues online
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail)
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment e.g trolling and stalking) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
- The safe use of social media and the internet will also be covered in other subjects where relevant.
- Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

V. Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training

The school will provide parents with training opportunism and online safety updates so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

VI. Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

- Any searching of pupils will be carried out in line with:
- The DfE's latest guidance on screening, searching and confiscation

UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

ADVICE TO STAFF

Searching a device

In a school-based context, it is highly likely that the image will have been created and potentially shared through mobile devices. It may be that the image is not on one single device: it may be on a website or on a multitude of devices; it may be on either a school-owned or personal device.

- If any illegal images of a child are found the police will be informed immediately.

Never…

- Search a mobile device even in response to an allegation or disclosure if this is likely to cause additional stress to the pupil UNLESS there is clear evidence to suggest that there is an immediate problem.
- Print out any material for evidence.
- Move any material from one storage device to another.

Always...

- Confiscate and secure the device(s)
- Inform the DSL.
- Record the incident on MyConcern as an 'online safety incident'
- Act in accordance with school safeguarding and child protection policies and procedures

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

VII. Acceptable use of the internet in school

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

The boundaries of use of ICT equipment and services is given in the Acceptable Use Statement; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

VIII. Pupils using mobile devices in school

The School operates a bring your own device (BYOD) system from Year 6, whereby pupil owned mobile devices, such as, smartphones, tablets, notebooks / laptops have the capability of utilising the school's wireless network. The device also has access to the wider internet and other cloud based services such as email and data storage via Microsoft Office 365. All pupils should understand that, during the course of the normal school day, the primary purpose of their device in a school context is educational. Boarders are permitted to use their devices for non-educational purposes outside of the normal school day. If there is reason to believe a pupil is misusing the privilege of having access to the School systems or internet the School reserves the right to access their accounts and if necessary suspend their access.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Further explanation on the use of mobile phones specifically is included in the Mobile Device Guidance section of this policy.

IX. Staff using mobile devices in School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates
- Staff members must not use the device in any way which would violate the school's terms of acceptable use
- Work devices must be used solely for work activities.
- If staff have any concerns over the security of their device, they must seek advice from the ICT Systems Manager

X. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on [behaviour and ICT and internet acceptable use – adapt according to what policies you have]. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

XI. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element
- Training will also help staff:
- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term
- The DSL and DDSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive updates from the DSL on safe internet use and online safeguarding issues.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

XII. Monitoring arrangements

- The DSL logs behaviour and safeguarding issues related to online safety via MyConcern.
- This policy will be reviewed every year. At every review, the policy will be shared with the governing body.

2. Staff Acceptable ICT Policy

I. Introduction

This important document sets out the school's policy with regard to use of the Internet and IT Systems by anyone other than a pupil. It should be read in conjunction with other policies – particularly policies and guidelines related to Safety/Child Protection. These can be found on the School's intranet. This policy applies to all non-pupil users of the school network, including teaching and administrative staff, children and partners of residential staff, visiting adults and children.

II. Security

The ICT Department publish clear guidance on password security on the intranet, and all staff are expected to adhere to this advice, and to make every effort to ensure the security of their password and access. Staff who are negligent in this regard may expect disciplinary sanction.

III. Internet

The Internet is provided by the school to facilitate you in your appointed role. The expectation is that in normal working hours your use of the internet is restricted to websites which contain information you require as part of your role in the school.

Outside working hours, as with pupil use, non-work-related surfing through school systems is regarded as acceptable, provided that the site:

- Does not contain illegal material
- Does not offer to violate or circumvent copyright laws
- Does not contain dubious or immoral material, in other words, material which a reasonable individual would consider to be inappropriate, including, but not limited to, pornographic, racist, sexist, blasphemous or violent material
- Is not a commercial site in which you have a financial interest
- Does not provide you with a means of contacting pupils directly (see below).

IV. Usage

The school would prefer you not to download non-work-related multimedia files, or listen to streaming audio or video. The school does not have the bandwidth available for these types of file download. Where you author or contribute to other websites, including blogs, forums or wikis, you should ensure that the site does not judge or defame the school or colleagues, and does not identify pupils either by name or in photographs unless the school holds written permission from the parents for such use. You are to log on only as yourself, and to keep your password secure.

Staff are not to share passwords with other members of staff, or their families. If your partner or children require access to the internet, please ask IT to provide additional logins which will not permit access to staff privileged data. Accidental access of inappropriate material should be reported to the appropriate member of the IT Department.

Attempts deliberately to access inappropriate material by employees or visitors through school systems would be regarded by the School as a significant breach of trust, or, for certain materials or sites, gross misconduct, which may result in the school taking disciplinary action.

Surfing is filtered heavily, in order to fulfil our duty of care with pupils. This filtering is also applied to staff surfing in order to prevent logins with enhanced privileges appealing to pupils. The School takes no responsibility for filtering web surfing for children of resident staff or visitors. Both in term-time and in holidays, the pages you visit are logged.

V. Contacting Pupils

If you need to contact pupils electronically you should normally use the school email system - the school system manages an "audit trail", for your protection, which is not necessarily present in other systems.

Do not respond to invitations from pupils in social networking sites.

Be aware of the professional risks involved in communicating with pupils via instant messaging, mobile phone, text messaging or other messaging type mediums, though the school recognises that there are situations, for example on school trips, emergencies, or where an immediate response is required, where there is no alternative.

A register of staff using social networks as part of their teaching is required. Please inform the Deputy Head Pastoral of

- name
- academic purpose
- pupils involved.

They must also delete those pupils no longer involved in the activity after that activity has ceased.

VI. School email addresses

These are to be used for school business only. Private use of your school email address is not advisable because the school keeps backup copies of your emails for your protection, and your folders may be moved to another member of staff, for example, when roles change.

The school may need to open your email and file folders for a variety of reasons, such as checks on incoming SPAM, access to an incoming email in your absence, or for disciplinary reasons.

If you forward your email to another account, take all reasonable steps to ensure that only you have access to the account, and the password access is secure. Consider carefully whether you need to forward. IT cannot be held responsible for any content you forward on to an account they have no control over.

If you read your school email at home, please ensure it is enabled on an account to which family members do not have access.

Do not use school email addresses to conduct a private business.

The sending of offensive or time-wasting email is forbidden. Indeed, it is illegal in some countries.

It is also advisable to archive your email from time to time to ensure the email systems work as effectively as possible. The IT Support team can advise on best practice.

VII. Data Storage, Access and Software

All school accounts have access to systems be they local or network based, which have the ability to store information/data or software.

The school expects that these data storage areas are used for the purpose of fulfilling your role whilst at Mount Kelly Foundation.

These areas must not be used to store personal data which is not school related or to install or run software which is not needed for work-based activities. Advice can be sought from the IT department for storage and backup of non-school related data.

The school stores sensitive information and some users may be granted access to this data. This data must not be copied, stored or moved in anyway which may identify, harm or breach any data protection policies. Where sensitive data is held each department or faculty should have a policy on how this data should be accessed and/or used if it does not adhere to present school data protection policies. In this regard advice should be sought from the IT Department.

All data stored on the network, for example your N: drive, is backed up. To ensure data backups can take place and run successfully, it is advised that only data which is used for academic learning and /or part of your role at Mount Kelly Foundation is stored on the network.

It is advised that storage of large media files such as photographs/videos and music be restricted to only those that are needed for teaching. Advice can be sort from the IT Support department if you require additional storage for these types of media.

It is also advised that departmental areas are used to store files and media to reduce data duplication; this also ensures all members of the department have access to the most up to date files.

For a variety of reasons the school may from time to time need to access user data, this will be managed in line with departmental or HR policies which are not included within this document.

Any person(s) who feel data protection has been breached should immediately inform the School Privacy Officer.

VIII. Use of Personal Equipment on the School Network

Use of personal equipment on the school network is permitted, however all devices should have no unlicensed or illegally copied software including music and other data files on it and you should be aware that you are still using school network systems to connect to the internet.

You are required to have installed and maintain an anti-virus-checking system to keep your computer free of viruses. Please contact IT Support if in doubt.

You may not run a server of any form on the school network – iTunes, Web, file, chat, news, mail. This includes "sharing files" with friends or colleagues over the network, without prior permission from the IT Department.

Wireless is permitted within residences but this must be secure and not made available to pupils; advice should be sought from the IT Department. Any additional network infrastructure added to the network to extend the use of the network within residential lets should be passed by the IT Department.

3. Pupil Mobile Device Usage

I. Introduction

The school recognises that mobile phones and digital devices are now an integral part of youth culture and can have considerable value, particularly in relation to individual safety and educational research. We recognise that such technology will play an increasing part in future learning practices, but, akin to wider ICT use, this should follow agreed rules and guidelines to prevent disruption and inculcate good learning habits.

Mobile phones do, however, present a number of problems:

They can disrupt the learning environment.

Their use can render pupils subject to potential bullying or inappropriate contacts.

Camera functions can lead to child protection and data protection issues with regard to inappropriate capture, use or distribution of images.

Phones / devices are valuable items that can be stolen.

Excessive mobile phone use can lead to a breakdown and degradation of social relationships.

The following restrictions therefore apply:

Pupils in Year 6 and below may not bring any mobile devices to School, unless with the explicit permission of a member of staff.

Pupils in Years 7 & 8 may bring laptops or iPads to school, in accordance with the Bring Your Own Device policy, but may not bring mobile phones.

Pupils in Years 9 to 13 are permitted to bring mobile phones and digital devices to school. Pupils in Years 9 to 11 lock their mobile phones in a Yondr pouch during the start of each day. This means that the pupil physically has the device, but has no way of accessing or using it.

Note: *The term 'phone' in this policy denotes mobile phones, IPods, MP3, MP4 players and any similar portable electronic devices.*

II. Responsible Use

- Pupils must ensure that files stored on their devices do not contain violent, degrading or offensive images.
- The transmission of some images/information can be a criminal offence and will be dealt with as such by the school and may involve handing the device over to the Police for investigation.
- Cyber-bullying is completely unacceptable, and will always be followed up by the school. *(See anti-bullying policy)*

III. Guidance for Parents

- Parents should only contact pupils at break times, lunchtime and after the school day has ended.
- In an emergency, parents are asked to phone Reception and/or the relevant Hm. A message will be relayed to the pupil.
- Responsibility for mobile devices rests with the pupil and the School accepts no responsibility for damage, loss or theft.
- In the event of pastoral difficulties or concerns, parents should consider whether direct communication with their son or daughter is necessarily helpful, or whether making contact first with the relevant Tutor or Hm might be more appropriate.

IV. Guidance for Pupils

- Appendix 3 sets out the Guidance for Acceptable Use of Mobile Phones.
- Pupils should understand that it is a privilege to be permitted to bring mobile devices to school and abuse of this privilege may lead to its curtailment.
- Pupils must not use devices during or between lessons, unless specific permission has been granted by the class teacher.
- If there is an emergency, or if a pupil feels unwell, which requires communication with home, pupils must speak to a member of staff who will assist with the matter.
- No device should be used in the School to photograph or video pupils or staff without their knowledge and permission.
- Headphones may not be worn during or between lessons, for reasons of safety and courtesy.
- Boarders found misusing phones / devices after lights out will incur sanctions as determined by the respective Hm.
- In the event of pastoral or disciplinary difficulty, or in the event of an emergency, pupils should not circumvent the school's processes and policies by ringing home immediately, but should, as a fist step, communicate with their Tutor, Hm or any other member of staff.

V. Phone Administration

- Details of the mobile phone number must be given to Hms at the beginning of term.
- Mobile phones cannot, under any circumstances, be taken into examination rooms. A breach of this rule will lead to invalidation of that examination and potentially other examinations.

VI. Sanctions

- A pupil found using their phone in such a way that constitutes bullying will be dealt with according to the Anti-Bullying Policy.

- Should a pupil in Years 9 to 13 contravene the Guidance set out in Appendix 3, the ‘phone or device will be confiscated and handed to Reception, from where the pupil may collect it at the end of the working day.
- Should a pupil have their phone confiscated for misuse in class, this will be recorded on iSAMS. Their phone will be handed by the member of staff either to Reception or to the pupil’s Hm who will discuss the matter with the pupil.

4. Social Media Policy

I. Introduction

The School recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers, and pupils are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the School, its staff, parents, carers, and children.

II. Scope

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the School.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education.
- Defines the monitoring of public social media activity pertaining to the School.

The School respects privacy and understands that staff and pupils may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the School's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account, or using the School name. All professional communications are within the scope of this policy.

Digital communications with pupils are also considered. Staff may use agreed social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.

III. Roles & responsibilities

SLT

- Facilitating training and guidance on Social Media use
- Developing and implementing the Social Media policy
- Taking a lead role in investigating any reported incidents
- Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
- Receive and manage and approve requests for Social Media accounts

Administrator / Moderator

- Create the account following SLT approval
- Store account details, including passwords securely

- Be involved in monitoring and contributing to the account
- Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)

Staff

- Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
- Attending appropriate training
- Regularly monitoring, updating, and managing content he/she has posted via school accounts
- Adding an appropriate disclaimer to personal accounts when naming the school

IV. Process for creating new accounts

Anyone wishing to create a new account must present a business case to the School Leadership Team which covers the following points:

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

V. Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention are essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

A member of the SLT will have administrator rights on any account associated with the School and will monitor accounts to ensure compliance with this policy and that posts are consistent with the purpose and values of the School.

VI. Behaviour

- The School requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and

privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the School.

- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff the member of staff should contact a member of the SLT immediately. They should not reply on behalf of the School.
- Unacceptable conduct, (e.g., defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the School and will be reported to the SLT.
- The use of social media by staff while at work may be monitored, in line with school policies. The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The School will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the School will deal with the matter internally. Where conduct is considered illegal, the School will report the matter to the police and other relevant external agencies and may act according to the disciplinary policy.

VII. Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

VIII. Handling abuse

- When acting on behalf of the School, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report, or delete other users or their comments/posts and should inform the audience exactly why the action was taken.
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

IX. Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g., Facebook)

X. Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the School's 'Use of Pupils' Images' policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload pupil pictures online other than via school owned social media accounts.
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Pupils should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

XI. Personal use

Staff

- Personal communications are those made via personal social media accounts. No personal accounts should link to the School and when posting on personal accounts it must be clear that you do not claim to represent the views of the School. Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school permits reasonable and appropriate access to private social media sites.

Pupils

- Staff are not permitted to follow or engage with current pupils and are strongly advised not to follow or engage with former pupils of the School on any personal social media network account.
- The School's education programme should enable the pupils to be safe and responsible users of social media.
- Pupils are encouraged to comment or post appropriately about the School. Any offensive or inappropriate comments will be resolved using the School's behaviour policy.

Parents/Carers

- If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
- The School has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
- Parents/Carers are encouraged to comment or post appropriately about the School. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the School's complaints procedures.
- Parents/Carers should be made aware of and adhere the points in Section 2 of the Use of Pupils' Images Policy.

XII. Monitoring posts about the School

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the School.
- The School should effectively respond to social media comments made by others according to a defined policy or process.

XIII. Advice for managing your personal use of Social Media

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Do not use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?

- Know how to report a problem

Managing school social media accounts

The Do’s

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views i.e., opinions are my own
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to ‘share’ other peoples’ materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school’s reporting process
- Consider turning off tagging people in images where possible

The Do Nots

- Do not make comments, post content or link to materials that will bring the school into disrepute
- Do not publish confidential or commercially sensitive material
- Do not breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and do not link to, embed, or add potentially inappropriate content
- Do not post derogatory, defamatory, offensive, harassing, or discriminatory content
- Do not use social media to air internal grievance

5. Streamed Media Policy

I. Introduction

Streamed video content, DVDs, and other digital video resources offer significant benefits in the classroom, offering depth and colour to the learning experience.

The use of such resources in lessons is not without difficulties, and this policy is intended to highlight the risks associated with this practice, and to provide guidance on safe and responsible use of digital media within the school. The document is not exhaustive and should be followed in line with other relevant school policies.

II. Context

There is a wide range of digital media available via the internet and other digital sources, but due to the dynamic nature of the internet there are risks associated with streamed media in particular, where content is uploaded by the general population and is largely unregulated. This presents issues with the validity of the content, potential copyright and other legal issues, as well as its appropriateness for the intended audience. Due to these risks, pupil access to these sites is regulated by the School.

Staff should also ensure that the video footage that they use in lessons (and more widely) is age-appropriate and within the classifications set by the British Board of Film Classification.

III. Guidelines

Staff using streamed and other digital media are expected to adhere to the ICT Acceptable Use Policy.

The primary purpose for using such media is to enhance teaching and learning within the school, or as part of our extra-curricular and pastoral provision – for example, within a boarding house.

Media content should be viewed from start to finish and a full assessment made of its suitability for the intended audience. The content should be considered in the same way that you would consider any other resources used in your classroom. Content must be assessed away from the view and earshot of students, preferably in a staff room or similar.

Many classroom PC's are connected to interactive whiteboards and projectors, and may be configured for whole-class display. This must be considered when reviewing content.

Particular note should be taken of the certification of any intended video content. The following guidelines apply:

• Nursery – Year 2	U certificates
• Year 3 – Year 6	U & PG certificates
• Year 7	U, PG &12A (with parental permission) certificates
• Years 8 & 9	U, PG, 12A &12 certificates
• Years 10 – 12	15 certificates
• Year 13	18 certificates

Staff should always err on the side of caution, and staff who wish to show video content to pupils that are under the prescribed age, parental permission should be sought.

IV. Unacceptable Use

It is deemed inappropriate to view, show, create, access, download or publish material that is:

- Pornographic or of an explicitly adult nature
- Racist, sexist, homophobic, or in any way offensive, or derogatory
- Obscene
- Bullying
- Violent
- Fraudulent
- Likely to cause harassment to others
- Confidential
- Prejudicial to the school's best interests
- Not relevant to the business of the school or governors
- Likely to irritate or waste the time of others
- Likely to breach copyright

It is accepted that the teaching of certain subjects may present the need to use resources that could fall into one or more of the above categories. In such situations it is expected that the subject matter is presented in context; in a sensitive, balanced manner; and that it is appropriate for the age of the intended audience. It may also be appropriate to warn pupils that they may find the content of the streamed media challenging.

V. Common Sense

As always, common sense should dictate the appropriate course of action, though the following guidelines must be adhered to:

- Pupils should never be left unattended watching streamed content.
- Should a member of staff inadvertently show digital content to pupils which they feel may breach the protocols set out above, they should immediately contact a member of the Prep or College SLT.

VI. Legal Risks

If staff view, create, access, download or publish material that is pornographic, libellous, defamatory, offensive, racist or obscene, they, the school and governing body may be held liable.

If staff unlawfully view, create, access, download or publish confidential or personal information, they, the school and governors may also be held liable.

If staff unlawfully or without permission view, create, access, download or publish material that is copyrighted, they, the school and governing body may be held liable for copyright infringement.

6. Use of Pupils’ Images Policy

I. Introduction

The Data Protection Act 1998 rarely applies in situations where photographs or videos are taken in schools. Where it does, the Information Commissioner’s Office (ICO), which oversees enforcement of the Act, has advocated a common-sense application of it. Where the Data Protection Act does apply, it will usually be enough for the photographer to ask for permission from the parent or individual to ensure compliance with the Act. Photos taken for official school use may be covered by the Act and pupils and students should be advised why they are being taken. Photos taken purely for personal use are exempt from the Act.

II. Image taking by parents, legal guardians or family members

- Parents, legal guardians, family members and friends can take images of their child and friends participating in school activities for family and personal use.
- All parents are to ensure that any images they take will not be used inappropriately, including being uploaded on social media sites.
- Photography and video filming is not permitted in the boarding Houses without the permission of the Houseparent.
- Use of cameras and other equipment will be monitored and Mount Kelly reserves the right to suspend their use at any time.
- If there is any doubt about any aspect of this policy, parents should contact a member of the SLT for clarification.

III. Images for school publications

- The School will only take and use images that are appropriate and are considered to not be open to misuse.
- All images of pupils will be held securely.
- Children will be made aware of why their picture is being taken and how it will be used.
- Children and parents will be given the option to not have their / their children’s images used if they are the sole focus of the picture.
- Children and parents are encouraged to recognise the value of group photographs or recordings of School events.
- Images of children from the School will not be used to illustrate controversial subjects.
- If a parent does not want their child’s image to be used in School publications, or materials, they must write in person to the Principal.

IV. Images for the school website

School websites are part of the internet and are more easily accessible than paper based School publications. The School will make sure that only appropriate images are used.

V. Webcams

Webcams are a useful tool for learning. They can allow an individual or class to interact over the internet with others and support links between pupils in different schools, countries and cultures.

A webcam will only be used in appropriate circumstances such as a normal class setting and both children and teachers will be made aware of when a webcam is in use.

The default setting, however, is that pupils engaged in remote learning will not have their cameras turned on.

VI. CCTV

The School uses CCTV in some areas of School property as a security measure.

Cameras will only be used in appropriate areas and there will be/is clear signage indicating where it is in operation.

VII. Children photographing one another

- Staff will supervise and maintain control as far as is reasonably possible of any photographic images taken by pupils.
- Mobile devices are less visible and can be used to bully or take inappropriate images. It is School policy to allow pupils to bring camera phones on site, but their use should not permitted in changing rooms, toilets or in other areas with a heightened expectation of privacy.
- If it is found that devices have been misused, the School will follow its usual disciplinary procedures.

Please note that images taken by the media are not covered by this policy and are subject to a separate set of regulations.

7. AI Policy

I. Professional Use: Planning and Administration

The primary goal of AI for staff is to reduce workload, but human professional judgment is always the final authority.

Mount Kelly operates within a secure Microsoft 365 environment. All AI use must occur through Microsoft Copilot for Education, using school accounts only.

Data processed by Copilot remains within Microsoft's secure tenant and is not used to train public AI models, ensuring GDPR compliance.

Independent use of AI is permitted for pupils only in Year 9 and above. Lower, Middle and Upper Prep should not have independent access in lessons, though teachers should demonstrate and develop AI.

The traffic light system below highlights suggested uses (green), areas to be cautious (amber), and prohibited uses (red). Always review outputs—do not assume AI is correct!

DO (Safe & Approved)	DON'T (Prohibited & Risky)
Use Copilot to draft quizzes, generate extension tasks, summarise documents, or create initial lesson structures.	Rely solely on AI to set objectives or sequence lessons. Always integrate your pedagogical expertise.
Ask Copilot to simplify a text, translate a passage, or generate diverse examples for differentiation.	Use AI-generated output without thorough review for factual errors, bias, or inappropriateness.
Use only school-approved AI tools as found in the intranet signed off by the DPO.	Input any confidential or sensitive information (student full names, grades, behaviour notes) into public-facing tools.
Use AI as a starting point to draft reports or rephrase feedback points.	Use AI to write entire reports or grade student work automatically without significant human oversight.
If AI significantly shapes a resource or plan, add a note like: (AI-assisted resource generation).	Claim AI-generated content as entirely your own work.

II. Student Use: Teaching and Assessment

AI use by pupils must be explicit, guided, and align with academic integrity. JCQ and IB provide examples of acceptable and prohibited AI use.

Fundamental Rule: AI is only allowed when specifically stated by the teacher for each assignment and to assist in workload.

When permitted (e.g., brainstorming, drafting, research): Teach AI literacy, insist on citation (tool, prompt, date, retrieval method), and design tasks requiring human analysis and reflection.

Example citation: Microsoft Copilot (2026). Generate a historical timeline of the Cold War. Retrieved 7 Jan 2026, from Microsoft 365 Copilot Service.

When prohibited: Formal assessments (GCSE, A-Level NEA/Coursework), substitution of AI-generated content as original work, and use by Year 7-8 without teacher-led demonstration.

III. Safeguarding and urgent incidents

Incident	Action
Potential AI Risk	Report immediately to DSL
Harmful Content	Close the device and contact DSL/SLT
Academic Misconduct	Secure evidence and escalate to Exams Officer/Head of Department.
Deepfakes / Impersonation	Secure files/URLs and report to DSL
Data Leak	If sensitive data entered into unauthorised AI, report to DH immediately
Wearable AI	Banned in school—request removal and inform DSL

8. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: Acceptable User Policy

This statement outlines what are acceptable and unacceptable uses of ICT facilities within Mount Kelly. It is relevant to pupils, staff, governors and visitors. Whilst we aim to support the full use of the vast educational potential of new technologies we also have a responsibility to provide safeguards against risk, unacceptable material and activities. These guidelines are designed to protect pupils, staff and visitors from online-safety incidents and promote a safe online-learning environment for pupils.

At Mount Kelly we believe that pupils should be trusted to use digital technologies in a principled and productive way. The general spirit of this policy is about giving everyone the opportunity to make appropriate and informed decisions regarding the ways in which they use digital technologies; we should all be fully engaged in the on-going debate about what responsible digital citizenship means and how we can nurture it within our school.

Examples of acceptable use are:

- Using web browsers to obtain information from the Internet
- Accessing databases for information as needed.
- Using e-mail and/or Microsoft Teams for business related communication.
- Using the school’s network to promote the exchange of information to further education and research and is consistent with the mission of the school.
- Using the school’s network to access outside resources that conform to this "Acceptable Use Policy".
- Using the network and Internet in a manner, which respects the rights and property of others.
- Keeping all accounts and passwords confidential and inaccessible to others.
- Following the school’s password creation advice for the creation of your own passwords.
- Showing responsibility by making backup copies of material critical to you.
- Showing responsibility by taking precautions to prevent malicious content on the school's equipment.
- Upon receipt of an attachment checking to making sure it is from a known source before opening the file/s.
- Backing out of an accidentally encountered site that contains materials that violate the rules of acceptable use, and notifying a teacher or supervising adult of the occurrence immediately.
- Logging out or locking computers when they are left unattended for any period of time.
- Recognise that electronic communications sent through or stored on the school’s network will be treated as school related and may be monitored or examined by the Head Master or his authorised delegates for operational, maintenance, compliance, auditing, security and/or investigative purposes.
- Reporting any damage to or loss of computer hardware immediately.

- Saving documents onto appropriate storage areas of the school network or other appropriate storage systems.
- Reporting any inappropriate behaviour and online bullying to the Principal Deputy Head or Deputy Head Pastoral.
- Take reasonable care that there is no damage or loss of any equipment on loan from school.
- Ensuring that access from an unsecure location (public Wi-Fi, unsecured Wi-Fi) from a school device utilises our VPN software.

Examples of unacceptable use are:

- Use of the Internet for purposes that are illegal, unethical, harmful to the school, or non-productive.
- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
- Recording, filming or take photographs on school premises without permission and with consent of the parent or guardian.
- Broadcasting e-mail, i.e., sending the same message to more than 20 recipients or more than one distribution list without permission from the Principal Deputy Head or Head of Prep.
- Relocating school information and communication equipment without prior permission
- Conducting a personal business using school resources.
- Transmitting any content that is offensive, harassing, or fraudulent.
- Using inappropriate language: do not swear, use vulgarities or sexual innuendos.
- The sending of material likely to be offensive or objectionable to recipients.
- Using programs that harass school users or infiltrate a computing system and/or damage the software components is prohibited.
- Changing original software setting/configuration of school owned computers.
- Doing harm to other people or their work.
- Do not install software on school computers unless authorised by the ICT Manager.
- Doing damage to the computer or the network in any way.
- Interfering with the operation of the network by installing illegal software, shareware, or freeware.
- Plagiarisation and violation of copyright laws.
- Conversation in email using all upper case letters. This is considered shouting.
- Sharing your passwords with another person. Doing so could compromise the security of your files.
- Wasting limited resources such as disk space or printing capacity.
- Trespassing in another’s folders, work, or files.

- Deleting any files in a shared directory which could still be required by others.
- Giving out personal information such as your home address or telephone number. Use the school's address instead.
- Viewing, sending, or displaying offensive messages or pictures.
- Accessing sites that contain pornography; that spread hatred; that promote discrimination; that give instruction for acts of terrorism, harassment, murder, suicide, or other illegal activity.
- Downloading files or content not required by the school using the schools internet connection without authorisation of the ICT Manager.

Appendix 2: Online Safety Training Needs – Self Audit for Staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school’s acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school’s acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school’s ICT systems?	
Are you familiar with the school’s approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	