



Myddelton College

Online and e-safety Policy

Policy produced by	Deputy Head Academic and DSP
Date policy reviewed and approved	January 2023
Reviewed and approved by	HT (LDA) and SLT Nov 2024
Reviewed and approved by	MPE/LDA Nov 2025 and Advisory Committee
Next review due	Nov 2026
Published on website	Yes No

MYDDLETON COLLEGE'S POLICY ON ONLINE / E-SAFETY

This policy statement should be read alongside our organisational policies and procedures, including:

- Safeguarding and Child Protection Policy
- Child on Child Abuse policy
- Anti-bullying Policy
- Managing allegations against staff and volunteers
- Code of Conduct for Staff
- Prevent Extremism Policy
- Photographs and Digital Images Policy

Regulatory framework in Wales, schools must follow:

- a. Keeping learners safe: the role of local authorities, governing bodies and proprietors of independent schools under the Education Act 2002 (Welsh Government, 2022)8.**
- b. Arrangements for safeguarding children are set out in section 175 of the Education Act 2002.**

This policy has also been prepared to meet Myddelton College's responsibilities under:

- The United Nations Convention on the Rights of the Child
- The Education (Independent School Standards) Regulations 2024;
- Boarding schools: national minimum standards (Department for Education (DfE), 2022);
- Education and Skills Act 2008;
- Children Act 1989;
- Childcare Act 2006;
- Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR);
- Equality Act 2010.

This policy also has regard to the following guidance and advice:

- Keeping children safe in education (DfE, September 2022) (KCSIE);
- Preventing and tackling bullying (DfE, July 2017);
- Sharing nudes and semi-nudes: advice for education settings working with children and young people (DCMS and UKCIS, December 2020);
- Prevent duty guidance for England and Wales (Home Office, April 2021)
- Channel duty guidance: protecting vulnerable people from being drawn into terrorism (Home Office, 2020);
- Searching, screening and confiscation: advice for schools (DfE, January 2018);
- Safeguarding children and protecting professionals in early years settings: online safety considerations (UK Council for Internet Safety, February 2019);

- Relationships Education, Relationships and Sex Education (RSE) and Health Education guidance (DfE, June 2019);
- Teaching online safety in schools (DfE, June 2019);
- Harmful online challenges and online hoaxes (DfE, February 2021)

1. Introduction

This internet or E-safety policy sets out and details of the school's responsibility to protect and educate pupils and staff in their use of technology and to have the mechanisms in place to intervene and support any incident where appropriate. This policy is available for all to read on the Myddelton College website.

Safeguarding is a serious matter; at Myddelton College, we use technology and the internet extensively across all areas of the curriculum. Online safeguarding, known as E-Safety, is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an E-safety incident, whichever is sooner.

The internet can be used for benefit:

- to improve communications, for banking, to shop and to pay bills, to obtain useful information, for entertainment and to understand other cultures.
- online education helps us to meet goals, can be used to improve teaching and learning, to undertake homework, to increase pupil engagement when learning, to improve retention, to increase independent learning opportunities and to develop life skills.

There are, however, negatives and we must ensure that these do not cause our pupils harm:

- the Internet can become addictive, it can allow some to obtain illegal or inappropriate information, our privacy can be put at risk, persons can be exploited, stalking could become easier, viruses could distort information and be used to our disadvantage.
- we have a duty of care to our pupils, protecting them from unsuitable content, illegal downloads, accidental disclosures of personal information and cyber-bullying, for example. Our pupils need to be aware that grooming, cyber-bullying and child radicalisation can be undertaken online.
- as adults, we must ensure we and those for whom we are responsible are not caught out by: phishing, scams, malware, worms, spyware, trojans, ransomware/scareware.

Where we discover illegal or even improper use of the internet, it is important we report both actual online abuse and/or concerns about the potential of online abuse to the school's Designated Safeguarding Lead and/or the Local Authority's Child Protection Team.

In practice, staying safe online is as much about behaviour as it is electronic security. When considering the possible ways in which young people in our care are at risk, the **Four Cs** are a good format to help shape our thinking:

- Content: being exposed to illegal, inappropriate or harmful material.
- Contact: being subjected to harmful online interaction with other users.
- Conduct: personal online behaviour that increases the likelihood of, or causes harm.
- Commercialism: being affected by advertising and marketing schemes, which can also mean inadvertently spending money online.

It is also important to consider how the **'Fifth C'** of Consent is involved with the areas above.

2. The purpose of this policy is twofold:

- a. To ensure the requirement to empower the whole school community with the knowledge to stay safe and remain risk free is met.
- b. To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

3. Awareness

All members of staff will be made aware of the policy, and the important role it plays in safeguarding pupils and staff, in both staff INSET meetings and when inducting new staff. They will be asked to confirm in writing they have read the policy, and will implement and abide by its conditions.

Pupils will be introduced to the policy in Year group assemblies and will discuss issues raised in PSHE classes for pupils. Every student must sign the ICT Acceptable Use Agreement before gaining access to the school's computer network and internet.

4. Specific roles:

a. Headteacher

Whilst the Headteacher has overall responsibility for Internet / E-safety within the school, the day-to-day management of this will be delegated to the E-Safety Officer.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the needs of pupils, all staff, senior leaders, Directors and parents.
- The E-Safety Officer has had appropriate CPD in order to undertake the day to day duties effectively.
- All E-safety incidents are dealt with promptly and appropriately.

b. E-Safety Officer (currently the Designated Safeguarding Person, Mr Mike Pearson)

The E-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher on all E-Safety matters.
- Engage with parents and the school community on E-Safety matters at school and/or at home.
- Liaise with IT technical support and other agencies as required.
- Retain overall responsibility for E-Safety incident reporting to the DSP and Headteacher
- Ensure any technical E-Safety measures in school (e.g. internet filtering software, behaviour management software) are fit for purpose.
- Be aware of any reporting function with technical E-Safety measures; this includes the internet filtering reporting function and liaison with the Headteacher to decide which reports are appropriate for viewing.

c. IT Technical Support Staff

They are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum: anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Software updates are regularly monitored and devices updated as appropriate. Any E-Safety technical solutions such as internet filtering are operating correctly.

- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the E-Safety officer and Headteacher.
- Passwords are applied correctly to all users. Passwords for staff will be a minimum of 8 characters with upper and lower case letters and numbers.
- The IT System has a secure password and access policy.

d. Teaching Staff

They should ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Every E-Safety incident is reported to the E-Safety Officer or in their absence to the Headteacher. If you are unsure the matter is to be raised with the E-Safety Officer or the Headteacher to make a decision.
- The reporting procedure is fully understood and implemented.

e. All pupils They must:

- * Read and implement the Pupil Acceptable Use Policy which explains the boundaries of use of ICT equipment and services in our school.
- * Recognise that any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.
- * Know that E-Safety is embedded in the curriculum - pupils will be given the appropriate advice and guidance by staff, in all subject areas across the curriculum.
- * Be fully aware how they can report areas of concern whilst at school or outside of school.

g. Parents and Carers

They should:

- * Play the most important role, that of oversight, supervision and control in their children's use of the internet; as such the school will provide parents with details relating to resources to acquire the skills and knowledge they need to ensure the safety of children outside the school environment.
- * At parents' evenings and in school newsletters, information relating to school Internet / E-Safety teaching will be given, and the availability of appropriate online training courses for parents will be provided to keep parents up to date with new and emerging e-safety risks. A highly recommended starting point for parents to use is the NSPCC website.

Parents will be encouraged to talk with their children about the safe use of the internet at home - in the evenings, weekends and holidays: this should be done to reassure children that parents are genuinely concerned about their safety and the risks involved in using the internet.

Questions might be linked to: Which apps do you use? Which websites do you use? Please will you show me ..." Parents need to be conversant with how the internet might be used to disadvantage; using the internet together is the safest way of ensuring appropriate use.

- * NSPCC training courses are available for parents and carers to follow, at different levels, to help parents and carers to develop appropriate knowledge and understanding of E-safety and the use of digital technology by their children. * The school will also involve parents in strategies to ensure that pupils are empowered to protect their privacy and safety.

5. Parents should also be aware that:

- The school needs have to rules in place to ensure that their children can be properly safeguarded.

- The School uses a range of devices including PC's, laptops and tablets. In order to safeguard the student and, in order to prevent loss of personal data, we employ the following assistive technology:

a. Internet Filtering:

We use a firewall product called Watchguard that filters and prevents unauthorised access to illegal websites, including those sites deemed inappropriate under the Prevent Agenda. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The E-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher. Web access is logged indefinitely for all users of the ICT systems available in School.

b. Email Filtering:

We use Forefront Office 365 technology that prevents any infected emails to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message. The system is also used to filter certain words and can be used for monitoring.

c. Passwords:

All staff and pupils will be unable to access the network without a unique username and password. Staff and student passwords should be changed if there is a suspicion that it has been compromised. The Network Manager will be responsible for ensuring that passwords are changed as and when required. The use of another person's credentials, at any time, is forbidden.

d. Anti-Virus:

All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns.

6. Applicability

Use of the school network, with access to the Internet, in school is a privilege, not a right.

All pupils will have access to a copy of this E-Safety Policy. Access to the network will be granted to new pupils upon signing and returning their acceptance of the Acceptable Use Policy.

These policies apply to all staff and pupils, including boarders, whether access to the school network or internet is by cable or wireless (or personal mobile account whilst on school premises, including school trips either in the UK or abroad) and on any device, laptop or PC, either school owned or personal.

7. Boarders

In the specific case of boarding, and at the discretion of the Head of Boarding and on advice from the Network Manager, the internet filters are changed to allow access to certain websites to boarders not available to pupils during the school day, primarily some social networking sites. This is in an attempt to replicate access to those sites non-boarders could reasonably expect at home during the week. Boarding staff monitor remotely the online activity of individual boarders during the evenings and the usual tracking and reporting logs, as used during the day, still maintained.

8. Social Media

For the purposes of this policy, social media is defined as interactive online media that allow parties to communicate instantly with one another or share information in a public forum. Examples include X, Facebook, Snapchat, Instagram and LinkedIn. Social media may also include blogs and video and image-sharing websites such as WordPress, YouTube and Flickr.

9. Email

All staff are reminded that emails are subject to Freedom of Information requests and, as such, the email service is expected to be used for professional work-based emails only. The use of personal email addresses for the purposes of contacting pupils is not permitted.

Pupils are permitted to use the school email system and, as such, will be given their own email address, based on their network user name. Pupils should use this email account only for school-based activity as laid out in the student Acceptable Use Policy that they have signed on entry to the school.

10. Photos and videos

Parents sign a photo release slip on entry to the school, as part of the Induction Pack they receive; non-return of the permission slip will not be assumed as acceptance.

11. Social Networking

Myddelton College is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community.

12. Pupil Images

With reference to images that may be uploaded to such sites, the following is to be strictly adhered to:

- a. Permission slips (either as hard copy filed in the student record folder or as flagged on the student record on **Engage**) must be consulted before an image or video of any child is uploaded.
- b. There is to be no identification of pupils using first name and surname; first name only is to be used, if at all.
- c. All images, videos and other visual resources that are not originated by the school are not allowed unless the owner's permission has been granted. Permission to use copyrighted resources must be received before used.

13. Notice and take down policy

Should it come to the school's attention that there is a resource which has been inadvertently uploaded, either to the school website or school/department authorised social networking sites, and the school does not have copyright permission to use that resource, it will be removed within one working day.

14. Reporting E-safety Incidents

Any E-Safety incident is to be brought to the immediate attention of the e-Safety Officer, or in their absence the Headteacher. The E-Safety Officer will assist in taking the appropriate action to deal with the incident and to fill out an incident log. All staff should make themselves aware of the procedures and the responsible staff involved in this process.

15. Training and Curriculum

It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using on-line digital technology; this includes updated awareness of new

and emerging issues. This includes the regular distribution of E-Safety information to staff, pupils and parents.

16. Staff training

In addition, Myddelton College will have an annual programme of online E-Safety training for teaching staff, to be incorporated within the CPD programme. This online E-Safety training will be renewed by further training on an annual basis. This continuous rolling training programme means that staff will always be up to date with the latest issues on E-Safety from new and evolving technologies.

17. The Curriculum

The school will ensure that aspects of E-Safety for pupils are firmly embedded into the curriculum. Whenever ICT is used in the school, staff will ensure that pupils are made aware about the safe use of technology and risks as part of the student's learning. If asked, Heads of Department should be able to demonstrate where and how the awareness of risk is imparted to pupils in lessons.

18. Required Training and Further Training

As well as the programme of training, the school will establish further training or lessons as necessary in response to any incidents.

The E-Safety Officer is responsible for recommending an annual programme of E-Safety training and awareness to the Headteacher for consideration and forward planning. Should any member of staff feel they have had inadequate or insufficient training generally, or in any particular area, this must be brought to the attention of the Headteacher for further CPD.

Currently the E-Safety Officer is Mr Michael Pearson, DHT (P) and DSP

Continuous Compliance and Best Practice Commitment

Myddelton College is committed to maintaining full compliance with Welsh Government statutory guidance and the National Minimum Standards for Boarding Schools. To strengthen this policy, the school will ensure that the latest Welsh safeguarding updates are embedded into annual staff and boarder training, and that risk assessments for emerging technologies are documented and reviewed regularly. In addition, the school will continue to monitor and evaluate technical safeguards, parental engagement strategies, and curriculum integration to ensure that online safety provision remains robust, proactive, and aligned with best practice.

Artificial Intelligence (AI) Awareness and Integration

Myddelton College recognises that AI technologies present significant advantages and potential disadvantages in education and wider school life. AI can enhance learning through personalised feedback, adaptive resources, and improved administrative efficiency. It also supports creativity and innovation in teaching and learning. However, the school is aware of associated risks, including data privacy concerns, algorithmic bias, misinformation, and over-reliance on automated systems. To address these, the policy ensures that AI use within the school is guided by principles of transparency, fairness, and safeguarding. AI tools will only be adopted following thorough risk assessments, compliance with UK GDPR, and alignment with safeguarding standards. Staff and pupils will receive guidance on responsible AI use, and any AI-driven decisions will remain subject to human oversight. The school will review AI-related practices annually to ensure they reflect best practice and emerging regulatory requirements.