The De Montfort School
E-safety Policy

Version Control
Policy author: Jayne Sampson
Policy approved by: Associate Headteacher
Next policy review date: Summer 2022

Version	Date	Details
1.0	18th March 2021	Creation of the E-safety policy (previously E-safety and student AUP)

This 'E-safety Policy' operates in conjunction with other policies-eg 'Behaviour Policy', 'Behaviour for Learning Protocols', 'Mobile phone, MP3 player and Games Console Policy' and 'Safeguarding Policy'.

Aim

We recognise the value of modern technology systems and welcome their development. We continually strive to enhance their appropriate use (both within school and outside) in order to promote the educational attainment of our students. This policy is of paramount importance as our students' access to technology is currently becoming universal and increasingly more mobile.

The technologies encompassed by this policy include all computer and internet technologies and electronic communication devices such as mobile phones and PDAs.

Any cases of a breach of the policy will be referred to the SLT member responsible for IT systems.

Internet usage

The internet is used within the school to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

We recognise the importance of the internet as an essential element in 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for students who show a responsible and mature approach to its use.

Students will use the internet outside of school and part of our responsibility is to educate them in safe use of the technology.

The breadth of issues classified within e-safety is considerable, but the three areas of risk we prioritise when talking to students are as follows:

- Content (being exposed to illegal, inappropriate or harmful material, extremist propaganda or any site promoting radicalisation).

Common risks we address with students within content focus on exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language) and substance abuse. We also focus on lifestyle websites, for example pro-anorexia/ self-harm/ suicide sites, and so-called "hate sites". Equally, we believe that it is important that students are taught to check the authenticity and accuracy of any online content they look at.

- Contact (being subjected to harmful online interaction with other users).

Dangers we address with students here include grooming, all forms of cyber-bullying, as well as identity theft (including so-called "frape", the hacking of Facebook profiles) and password security.

- Conduct (personal online behaviour that increases the likelihood of, or causes harm).

Within this area, students are taught about privacy issues, including disclosure of personal information, as well as digital footprint and online reputation. They are also taught about the need to consider health and well-being, where necessary limiting the amount of time spent online (internet or gaming). Equally, we believe it is important that students are educated about the dangers of sending or receiving personally intimate images, and of infringing music and film copyright laws.

Use of the internet within the school

Amongst the uses of the internet within school are the following:

- Access to learning wherever and whenever convenient.

- Access to world-wide educational resources including museums and art galleries.
- Educational and cultural exchanges between students world-wide.
- Access to experts in many fields for students and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Exchange of curriculum and administration data with the Local Authority and DfE.

Student safety on the school internet system

- The school internet facility has been designed expressly for student use and includes filtering (Smoothwall) appropriate to the age of students.
- Students are taught what internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning activities.
- Staff guide students in on-line activities that will support learning outcomes and plan for the students' age and maturity.
- Students are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Gaining access to the school internet

- The school maintain a current record of all system users (including staff and students) who are granted internet access.
- All students must read and accept the 'Student ICT Acceptable use policy' before using any school ICT resource.

Inappropriate usage of internet and loss of privilege

Any student in breach of the agreement for usage of the Internet will have their access curtailed immediately pending an investigation.

Social Networking services

Access to Social Networking services (for example Twitter, YouTube, Facebook, Instagram, Snapchat, Pinterest and Tumblr) is forbidden in school and all such sites are blocked. Students using such sites outside of school have a duty to use them responsibly. Any incident of slander, abuse or defamation perpetrated on a social networking site which impacts upon one of our students, shall be treated as bullying and shall be sanctioned in accordance with the school's behaviour policy.

Mobile Phones, Game consoles and other hand held electronic devices

It is our policy to allow students to have a mobile phone with them in school should they choose to do so under the conditions outlined in the 'Mobile phone, MP3 player and Games Console' policy.

School website

The contact details on the website are the school address, e-mail and telephone number. Student personal information is not and shall not be published.

Publishing students' images and work

- Photographs that include students will be selected carefully and will be appropriate for the context.
- Students' full names will only be used when featured on news articles sent to press.
- No photographs of students are published on the school website without permission from the parent/carer.
- Student work can only be published with the permission of the student.

Information system security

- School ICT systems' capacity and security are reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

Protecting personal data

Personal data is recorded, processed, transferred and made available according to the General Data Protection Regulation.

Assessing risks

The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school can accept no liability for the material accessed, or any consequences of Internet access.

Handling e-safety complaints

- Any complaint about student misuse must be referred to the SLT member responsible for IT systems in the first instance.
- Complaints of a child protection nature must be dealt with in accordance with the school's safeguarding procedures.

Communication of Policy

- Students are informed that internet use will be monitored.
- Students are asked to read and accept the Student ICT Acceptable Use Policy before accessing the network.

Information and guidance

We offer all our students a wide variety of ICT resources which are under constant improvement and development. They are offered access to The De Montfort School network, internet and electronic mail (email). Keeping our students 'safe' on the internet and supporting them to use the network appropriately is one of our key responsibilities. As a consequence, we operate a 'Student ICT Acceptable Use Policy' and hope that parents/carers will support us. The 'Student ICT Acceptable Use Policy' will be explained to all new students during their first 2 weeks in school and then reiterated annually. Access to The De Montfort School network, internet and electronic mail (email) will stop once students have left the school.

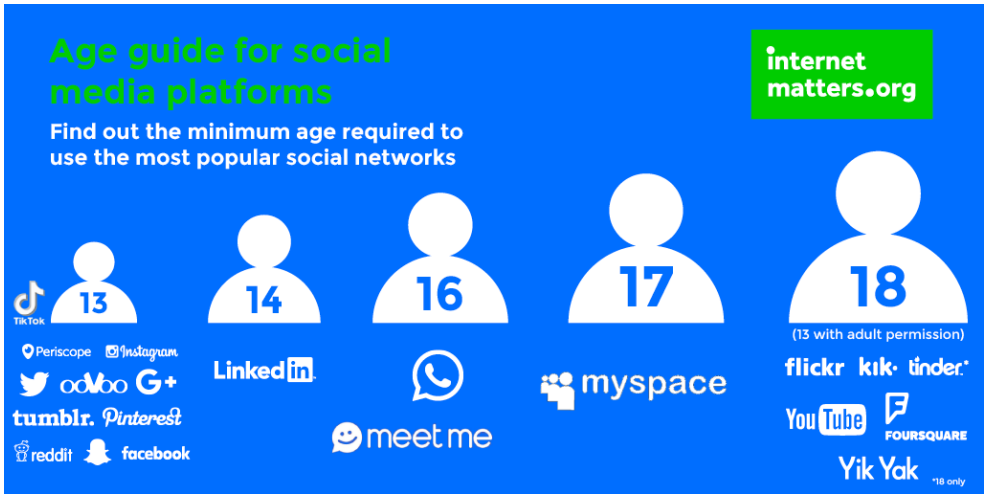
At the outset we must emphasise that the majority of our students use the network, internet and electronic mail (email) safely and sensibly and this document acts to increase awareness for all. We take any infringement of the 'Student ICT Acceptable Use Policy' very seriously and have installed software to monitor the use of the network, internet and email. Any case reported will be thoroughly investigated and judged on an individual basis. Students should expect serious sanctions to apply.

As part of the school's ICT programme, we offer students supervised access to the internet. Before the school allows students to use the internet, they must obtain permission from their parent/carer. Various projects have proven the educational benefits of internet access, which enables students to explore thousands of libraries, databases, and bulletin boards. They will also be able to exchange messages with other learners throughout the world.

It is the school's policy that every reasonable step should be taken to prevent exposure of students to undesirable materials/contacts on the internet, including extremist propaganda or any site promoting radicalisation of any sort. It is recognised that this can happen not only through deliberate searching for such materials, but also unintentionally when a justifiable internet search yields unexpected results. To reduce such occurrences, the school has its own dedicated broadband line and filter (Smoothwall). This facility stops students accessing sites deemed inappropriate for use at school and also provides a full audit trail. We believe that the benefits to students from access to the internet exceed any disadvantages. However, as with any other area, parents/carers are responsible for setting and conveying the standards that their sons/daughters should follow when using media and information sources. The school therefore supports and respects each family's right to decide whether or not to apply for access. During school, teachers will guide students towards appropriate material. At home, families bear the same responsibility for guidance as they exercise with other information sources such as television, telephones, films and radio.

YouTube, Instagram, Snapchat, Facebook, Twitter, Pinterest and Tiktok These are the names of well-known and popular websites many people - adults and children - will probably have come across. When used positively they allow people to share music, video, art, opinion, collaborate on work or indeed just have social discussions. Most of the content is harmless; other content can be cruel and cutting. The sites are not rigorously censored in terms of content. For example, on YouTube the BBC is putting video trailers for its forthcoming TV programmes whilst other contributors are posting more material that is inappropriate. The other sites allow 'members' to write about themselves, and other people of course and not all of it is appropriate.

Anyone can view the content on YouTube, although for access to some sites users have to register details on the site. Access to these sites is very easy. For students, having their own 'social networking' space is a very popular thing to have, but both parents/carers and students are not always aware of the risks they face when using sites like Facebook, Instagram or Snapchat. One of the rules that you may not be aware of is the minimum age for the sites such as Facebook is 13. Please see the graphic below for the age restrictions for different social media platforms.



It is worth remembering that these are public spaces and so anyone can view and use the information how they please. Your son/daughter may already be a member of them and a contributor, not just a reader of material. That means they have access to material, which you may well consider inappropriate. The users of these sites have the ability to create their own material and post whatever they like on to their site i.e. films, images or text. As it is accessed solely by user identification and a password, it is their choice who views it and whom they choose to pass it to. Here are the main e-safety issues, which should be discussed with your son/daughter:

- Personal Identity Fraud: there is a concern if students post personal details or complete online surveys. They should avoid giving out their full name, mailing address, telephone number, the name of their school, or any other information that could help someone determine their actual identity.
- Public Domain Information: all images, comments are stored and made available to the public. There are privacy settings and they should be used.
- Online Bullying: this can be in the form of comments, blog entries and chat rooms. Students must not send, share and upload of images, photos or videos that:
  - are illegal, obscene, defamatory;
  - bring the school into disrepute or
  - are intended to annoy or intimidate another person.
- Exploitation/ Misrepresentation: clearly people may try to make contact with students and they may not be who they say they are. Students should never meet anyone they have met online.

You know your son/daughter best. Visit the sites and see for yourself what's being said and the potential of what could be said or shown. Ask your son/daughter if they use the sites at all. If so you might engage in a discussion with them about the issues we have highlighted above. The websites can be useful and are a part of life nowadays. However, educating our children on the issues will mean they can use them safely.

Electronic mail (email) provides a quick and effective means of communication. Students must be made aware that they will be held responsible for the content of any email message they transmit and that they should not contain messages using language or content that is unacceptable. It is also recognised that some people may try to use email to identify and contact students for unacceptable reasons.

To avoid these problems the school has adopted the Local Authority's system for filtering all emails sent or received. The following points should be supported at all times:

- Steps should be taken to verify the identity of any school, organisation, adult or child seeking to establish regular email with the school or its students.
- Students should avoid revealing their identification within email messages. Students should only be identified by their network username and the student's own address is never revealed.
- Information should never be given that might reveal a student's identity or their current whereabouts.

We also have a number of leaflets from national bodies that explain issues further and also cover internet use at home. If you would like copies of these, please contact the school. Further information about e-safety can be found at

www.thinkuknow.co.uk	General online safety
www.chatdanger.com	Using chat rooms, mobile phones and email safely
www.blogsafety.com	Using blogs and social networking

This document aims to outline the key aspects of using the ICT facilities but if you require any further advice please contact the school.

Student live online lesson code of conduct

This code of conduct outlines how we expect you to behave when you are learning online. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything you do on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep you safe. You should not behave any differently when you are out of school or using your own device or home network.

1. To ensure that my studies are not disrupted because I am temporarily working away from school, I give permission for my school email to be used by my teachers for teaching and learning purposes.
2. I will treat myself and others with respect at all times; when I am online or using a device, I will treat everyone as if I were talking to them face to face in a classroom.
3. I will ensure my parent/carer is aware of when the live online lessons are taking place.
4. The messages I send, or information I upload, will always be polite and sensible. I understand that all messages I send reflect on me and the school.
5. I will choose a sensible place to work from – ideally a living room - and I will dress appropriately for my lessons as I would do at school.
6. I will make sure that I have all the tools I need in advance, so that I do not have to leave my desk and interrupt the flow of the lesson.
7. I will be at my online lesson on time.
8. I will complete exercises as directed by my teacher and upload completed work to meet the deadlines set by my teacher.
9. I understand that my online lessons may be monitored by senior leaders from the school.
10. I understand that MS Teams and Google Classroom is a closed school system open to me through the school's network and is limited to me, the staff and my fellow students. I should not invite any guests from outside the school to join the system through the use of my login details.
11. I will not under any circumstances provide my login details to anyone else. The system is fully secured and my activity on the system can be monitored.
12. I will be careful when opening and sharing files and attachments, checking for viruses etc. If I am unsure I will never open a file, hyperlink or any other attachment.
13. I will not share my or others' personal information that can be used to identify me, other students or my teachers on any online space, unless a trusted adult has given permission or reviewed the site.
14. I will never take secret photos, recordings or videos of teachers or other students.
15. I understand that all online lessons will be recorded in order to protect me and the teacher.
16. I understand that there may be two teachers present in the lesson in order to protect me and the lead teacher.
17. I will join the lessons at the times I have been given and if I am unable to join the session for any reason e.g. through ill health, I will let my teacher know in advance.

You will be asked to complete an agreement form to say that you have read and understood the code of conduct. No student will be given access to live online lessons without a completed agreement form.

ICT Acceptable Use Policy for Students

Aims
The aims of this Acceptable Use Policy are:
- To ensure that students may benefit from the learning opportunities offered by the school's network and internet resources in a safe and effective manner.
- To protect the school's ICT infrastructure from misuse and attack.

The school undertakes to:
- Prioritise Data Protection and adhere to strict guidelines on the use of personal or sensitive information.
- Provide a safe and productive digital learning environment
- Provide students with training in the area of internet safety
- Supervise students' network and internet access wherever possible
- Monitor students' network and internet activities using software systems
- Provide internet filtering (Smoothwall) in order to minimise the risk to inappropriate material
- Ensure there is a secure and regular backup of student data wherever possible. Nevertheless, students are still primarily responsible for backing up their own data and work.
- Ensure that robust and up to date virus detection and security systems are in place to protect students' data.
- Only publish students' projects, artwork or school work on the School Website/Internet in line with agreed school policy.

Important information for all students:
- Use of ICT Facilities is forbidden unless supervised by a member of staff
- Network and Internet use and access is considered a school resource and a privilege
- If the school AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions will be imposed.
- Designated staff can review student files and communications to ensure that the system is being used responsibly. They also have the right to access computer storage areas, accounts and removable media, including USB Flash Drives and CD-ROMs
- Designated members of staff can remotely view a student's computer screen at any time, without them knowing, in order to ensure compliance and appropriate use of The De Montfort School network.
- Students are subject to the provisions of the Copyright, Designs and Patents Act 1988;
- The school will provide information on the following legislation relating to use of The De Montfort School network, which teachers, students and parents/carers should familiarise themselves with: The Data Protection Act 2018; Video Recordings Act 1989; Copyright, Designs and Patents Act 1988; and Computer Misuse Act 1990.

Students will:

- Always keep passwords a secret.
- Only contact members of The De Montfort School staff via the school email system, Google Classroom or via the chat function in Microsoft Teams.
- Observe good etiquette at all times and behave in a way that reflects well on them and the school.
- Use The De Montfort School network for school related matters only, use computers for educational purposes and adhere to the student print policy.
- Make sure they take regular backups of their work.
- Respect other computer users and never harass, harm, cause insult or offence.
- Respect the security protocols in place on the computers and not attempt to bypass or alter security settings put in place on The De Montfort School network. Attempting to bypass or breach the school security systems is a serious offence.
- Use approved school email accounts for school use only. Personal email accounts such as hotmail and gmail are prohibited.
- Only use discussion forums or other electronic communications that have been approved by the school.
- Report any damaged ICT equipment (accidentally or otherwise) to the supervising member of staff immediately.
- Read and adhere to school information on e-Safety, cyber-bullying and social networking guidance.
- Read and adhere to the rules set out in the 'Student live online lessons code of conduct'.
- Always ask for permission to use the printer and will not print unnecessarily. I also understand that any print jobs I send to the printers are monitored and recorded.
- Take personal responsibility to check the copyright status of any material that I obtain from the internet, or post on to the internet.
- only use the internet for educational purposes. I will not use it for financial gain, for gambling or for advertising.
- I will report any attempts to contact me by people outside the school community to a member of staff.
- will not attempt to release viruses, or carry out any other malicious practice that contravenes the Computer Misuse Act 1990.
- I am aware of the CEOP report button and know when to use it.

Students will NOT:

- Contact any member of The De Montfort School staff via social media.
- Use USB sticks or portable memory devices in school.
- Attempt to upload, download or transfer any software from the internet or portable media.
- Attempt to bypass the school's internet filters (Smoothwall). Violation of this is a serious offence.
- Copy software or multimedia content unless it has been approved by a member of staff.
- Install, attempt to install, or store programs of any type on The De Montfort School network.
- Use the internet, computer systems, portable media or other mobile devices for playing non-educational games.
- Store personal photographs, music, games or other prohibited/inappropriate content in their user area (U: Drive) or anywhere on the school network.
- Damage, disable, dismantle or otherwise cause, or attempt to cause harm to the operation of computers, or any other ICT equipment or cables.
- Attempt to connect mobile equipment (e.g. laptops, tablets, games consoles, mobile phones etc.) to the school network.
- Eat or drink in any room where there is ICT equipment.
- Reveal their password to anyone, or use someone else's username or password. Students are responsible for the actions of anyone who is using their username and password, so must immediately tell a member of staff if they suspect that someone else has this information.
- Access or alter other people's folders, work or files without permission.
- Visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials, including any website containing any form of extremist propaganda or promotion of radicalisation. Any such sites should be reported to a member of staff immediately.
- Send, receive, share or upload any material that:
  - is illegal, obscene, defamatory;
  - brings the school into disrepute or
  - is intended to annoy or intimidate another person.
- Use social networking sites, such as Twitter or Facebook while in school, or use such platforms to make public comments about The De Montfort School, its staff or students, which are defamatory, liable to cause offense or bring the school into disrepute.
- Pass personal information on (like real names or addresses) to anyone on the internet.

Additionally, when using a computer:

- Always keep your personal details private (your name, family information, journey to school, are all examples of personal details) and never post these on a website.
- Never meet an online friend without taking a responsible adult that you know with you, and don't befriend people you do not know. Not everyone online is who they say they are.
- Do not post any pictures online that staff, or your parents may consider to be inappropriate. Remember, once you upload a picture on to the internet, most people will be able to see and download it. It's not yours anymore.
- Do not respond to any messages that are mean or in any way make you feel uncomfortable. Let a member of staff know if you are receiving such messages. I will also be polite and responsible when I communicate with others
- Do not use bad language or other inappropriate languages in any communications (eg. emails and other documents). This also includes homophobic, racist and other abusive messages.

Using School Laptops and Chromebooks at Home

In some circumstances, students may be allowed to borrow school laptops or other ICT equipment. The student and parent/carer will need to sign a document to accept responsibility of the device. All devices must be returned to the school once the student leaves, when the student no longer needs it, or when it is requested back by a member of staff.

- You will not leave the device unattended and it must be securely stored when not in use.
- You will not install any software on the device without consulting the TDMS Tech Team first.
- Any technical issues with the device must be reported immediately to a member of the TDMS Tech Team. Students MUST NOT attempt to disassemble the device or attempt to fix it themselves.
- If you lose your device, or if it is stolen, you must report it immediately to your form teacher, or a member of the ICT Tech.
- If you accidently damage the device, you must report it immediately to your form teacher, or a member of the ICT Tech Team.
- No modifications will be made to the device. All hardware changes and installations must be completed by a member of the ICT Tech Team.
- The device is to be used for educational purposes only.
- It is recommended that data stored on the device is backed up in to your Google Drive regularly. Should an issue develop with the device, the ICT Tech Team may be required to reset the device to its original factory settings. Such a procedure will result in the irretrievable loss of all information stored on the device.

While the device remains school property, the usage of the device will be monitored

On acceptance of the device, the student and parent/carer accept responsibility for the safe keeping of the device and if it is damaged beyond repair or lost they will be invoiced for the full cost of the replacement.