Online Safety (sections of the policy with relevance to parent/carers & students at MCC)

Students

Students are responsible for using the College IT systems and their own personal devices when in College as outlined in accordance with Appendix B, Acceptable Use Policy. All students have seen and understood the expectations of the College and therefore when accessing our systems, or using personal devices on College site are agreeing to follow these expectations. It is important that students:

- Understand that their Online behaviour may be addressed if it breaches any elements of the Acceptable Use cited in Appendix B. This includes inappropriate searches.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. Including the expectations around Generative AI as outlined in Appendix D.
- Will be expected to know and understand the College rules on the use of mobile phones, digital cameras and hand held devices.
- Government guidance is clear that mobile phones should be prohibited in schools. However, we will allow mobile phones within our setting, as long as they are switched off and not seen, unless they have express permission from a staff member. Any mobile phones will be confiscated for not following this instruction.
- They should know and understand College policies on the taking / use of images, audio or video recording and on cyber-bullying.
- Should understand the importance of adopting good Online Safety practice when using digital technologies out of College.
- If using a College owned device that they comply with Appendix C the 'Home Loan agreement'.

Parents / Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and or digital devices safely. It is important that they are vigilant in checking and monitoring the use of such technology at home and reporting and sharing any concerns with the most appropriate organisation e.g. the Police, CEOP.

The College will take every opportunity to help parents/carers understand these issues by distributing information on our website and signposting any national / local Online Safety campaigns / literature.

Parents/Carers will be responsible for ensuring that their child knows to follow the conditions of this Policy, in particular Appendix B, and to support the College when action needs to be taken e.g. the use of sanctions and/or referrals both internally and externally. These actions are taken to ensure that all College users are protected.

Parents/Carers are expected to support the College by ensuring that:

- They are educating their child to be a responsible user of electronic devices and the Internet in all aspects of their life. This does include checking the legal age and requirements for your child to use apps, games and any other social media or online activity ensuring that they are not accessing these if they shouldn't be.
- Ensuring that their child is not making derogatory comments towards others, which includes cyber bullying, and causing upset to others which may be due to harassment; inappropriate use of digital images, videos, including using images of others where consent has not been given; sharing upsetting material with others which causes distress.
- Being aware and reinforcing with your child that any deliberate misuse or breakage of equipment which impacts on the effectiveness of College IT systems, equally any activity which could put the security of the systems and users at risk, will be investigated and sanctioned as deemed appropriate by the College. If it is a believed a crime has been committed this will result in a referral to the police and or other agencies.
- That you are involved in the education and guidance of your child with regard to their on-line behaviour. This may include delicate subjects such as youth self generated images, the sharing of nudes or semi nudes, and avoiding inappropriate / age related material on the internet such as pornography, gambling etc.
- Being aware that personal devices may be confiscated as they potential contain evidence or child abuse material that may need to be passed on to other agencies e.g. the police.
- If their child is using a College owned device external to College, that they are responsible for complying with Appendix C the 'Home Loan agreement' and it's appropriate use as the College are unable to enforce the usage, filtering, monitoring and security of the device.

The College takes all incidents of misuse of IT or social media very seriously and if appropriate will refer serious incidents to the police in line with the Malicious Communication Act.

Please be aware that this applies to the activities of parents/carers online where statements are made that could bring the College into disrepute or may cause offense or upset to other College members which includes staff or students. Legal action will be pursued if defamation of character occurs online and by other media channels.

As part of the enrolment of your child at Minsthorpe Community College you agree to the conditions set out within this policy and will support the College in ensuring that all College users are not at risk.

Section 4

Education

Students

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

Online Safety education will be provided in the following ways:

- A planned Online Safety programme will be provided as part of IT / L4L / pastoral curriculum & other lessons and should be regularly revisited – this will cover both the use of IT and new technologies. This will also encompass the moral issues that students should consider when using these technologies.
- Key Online Safety messages will be reinforced as part of a planned programme.
- Students will be taught in lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information (misinformation, disinformation & conspiracy theories can cause safeguarding harm)
- Students will be helped to understand the need for the student acceptable use (Appendix B) and encouraged to adopt safe and responsible use of IT, the internet and mobile devices both within and outside College
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff will act as good role models in their use of IT, the internet and mobile devices

Parents / Carers

Parents and carers may have a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

The College will therefore seek to provide information and awareness to parents and carers via the website and they are also available to discuss any concerns, issues that they may have with the key staff indicated within this policy and or Head of Year.

Section 7

Use of Video, Audio, Digital Images and Recordings

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images or recordings on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The College will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- In accordance with UK GDPR, a student under the age of twelve is unable to give consent for their image to be used. It is for this reason that we seek the consent of parents/carers as part of the admission process and this data is held on Internal College systems.
- Once a student has reached the age of 12 they are deemed old enough to give consent themselves however staff should check whether consent was given before capturing any digital content and liaise with the Administration Team to gain consent if needed.
- For safeguarding purposes, staff are required to notify students when they intend to photograph / film / record during an activity. Staff should make it clear to the students the purpose of the digital images / recording and respect the wishes of any student who does not want to be photographed / filmed / recorded.
- When using digital images or recordings, staff should inform and educate students about the risks associated with the taking, using, sharing, publication and distribution. In particular, they should recognise the risks attached to publishing their own images or recordings on the internet e.g. on social networking sites.
- Staff should make every attempt to use college devices only to take any digital footage of students. Where this is not possible (and only with the express permission from the Leadership Team) staff must ensure that any data e.g. Image, video etc. should be transferred to the College systems as a matter of

urgency and at the earliest opportunity and then immediately deleted from their personal device.

- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the College into disrepute.
- Students must not take, use, share, publish or distribute images, audio or video of others without their permission. Students must adhere to the college policy when attending after college events, clubs or sporting events and may only use phones or other digital devices to take images / recordings with the express permission of the lead member of staff.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, in association with photographs
- Written permission from parents or carers will be obtained before photographs of students are published on the College website or other publications if under 12 years old.
- Student's work can only be published with the permission of the student or parents / carers.
- We may use group or class photographs or footage with very general labels, such as 'a science lesson' or 'textiles lesson'.

Section 10

Communication

The College considers the following as good practice:

- Staff will only communicate with student's using official College email, Satchel One or other College systems. These systems are safe, secure and are monitored.
- Students should therefore be aware that staff will only respond to communication via these systems and students must only use their College email to communicate with staff.
- All Users need to be aware that email communications will be monitored.
- Students should report any concerns to their class teacher or Head of Safeguarding.
- Staff must immediately report any Concerns to the Assistant Principal for Student Safety and Wellbeing or the Director of HR about the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to or delete any such email.

- Any digital communication between staff, students or parents/carers must be professional in tone and content. These communications may only take place on official College systems. Personal email addresses, text messaging or public chat / social networking programmes should not be used for these communications.
- Students will be taught about appropriate communication and risks attached. They will also be taught strategies to deal with inappropriate communications and will be reminded as part of the College's Online Safety program of the need to write clearly and correctly and not include any unsuitable or abusive material.
- Personal information will not be posted on the College website and only official email addresses will be used to identify members of staff.
- Mobile phones in Schools guidance has been considered and updates to the policy have been made in reflection of this communication tool.

Section 11

Inappropriate Activities

Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

Child sexual abuse/ intimate image abuse/ sexual exploitation
Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation; exploitation in any format i.e. trafficking
Adult material that potentially breaches the Obscene Publications Act in the UK
Criminally racist material in the UK
Pornography
Promotion of any kind of discrimination (in line with protected characteristics)
Promotion of racial or religious hatred
Threatening behaviour including: promotion of physical violence or mental harm; inciting violence; extreme violence; terrorism
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the College or brings the College into disrepute
Using College systems to run a private business
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the College
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)

Creating or propagating computer viruses or other harmful files
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
On-line gaming
On-line shopping / commerce/ selling any goods via school systems/devices
Unlicensed file sharing, e.g. of music, recordings, files, videos
Use of social networking sites unless authorised
Use of video broadcasting e.g. YouTube without express permission of staff for educational purposes

The College will only deal with incidents that involve inappropriate rather than illegal misuse. Any incidents of Illegal misuse will be reported to the appropriate service provider and or the police.

It is important that any incidents are dealt with as soon as possible in a proportionate manner and these will be dealt with through normal behaviour procedures.

Staff should be vigilant for the following examples of IT misuse:

Malicious use of social media
Deliberately accessing or trying to access material that could be considered inappropriate without an educational purpose
Unauthorised use of non-educational sites during lessons
Unauthorised use of digital devices on College site
Unauthorised downloading or uploading of files
Allowing others to access College network by sharing username and passwords
Attempting to access or accessing the College network, using another student's / student's account
Attempting to access or accessing the College network, using the account of a member of staff
Corrupting or destroying the data of other users

Appendix B

Student Acceptable User Policy

Student Responsibilities	
Username and password	I will not share my username and/or password, nor will I try to use any other person's username and password.
Personal Information	I will not share personal information about myself or others when online.
Reporting	I will immediately report any unpleasant or upsetting (inappropriate) material or anything that makes me feel uncomfortable when I see it to the service provider, Online reporting tools a trusted adult or teacher.
Device use	I understand that the college IT systems are primarily intended for educational use and that I will not use the systems for personal use unless I have permission from a member of staff to do so.
Internet searches/Gaming / Streaming / Gambling	I will not use the college IT systems for on-line gaming, on-line gambling, internet shopping, or streaming. I understand that the College will monitor my searches and sanctions may be applied if I do not meet this expectation.
Malicious damage and theft	I will not steal, disable or cause any damage to college equipment, or the equipment belonging to others.
Respecting others work	I will respect others' work and property and will not access, copy, delete or alter any other user's files, without permission. I should ensure that if I use the original work of others in my own work, I have permission to do so.
Communication	I will be polite and formal when I communicate with others.
Personal Devices	I will only use my personal device in college if I have express permission from a member of staff and am logged on to the college Wifi. Failure to follow the above will result in confiscation of my device. I understand that the safety of my personal device is my responsibility and not that of the college.
Recording others	I will not take photos; record videos or sound clips of others without express permission from a staff member
Security	I will not try to upload / download or try to access any materials that are inappropriate or illegal, or use software that will allow me to bypass the college security put in place.
Outside of College	I will not make negative comments or post upsetting material which will cause distress to other college users e.g. other students or staff. This includes content posted via social media and other apps.
AI	I will not use AI for any purposes other than education as directed by staff at the college.
College Responsibilities to students:	
Monitoring & filtering	It's the responsibility of the college to monitor and filter access to all IT systems and digital communications and ensure security of our

	systems whilst on our site. Therefore, students must use the College Wifi as directed above.
Security	It is the responsibility of the college to provide a safe and secure IT environment for all users when on our site.
Education	It is the responsibility of the college to make sure that students are aware of their responsibilities online and to help them to become better online users.

Please note that by logging on / signing into our IT systems you are accepting the terms and conditions laid out in this Online Policy.
It is important to understand that failing to follow these conditions will result in any follow up actions that are needed which may include College sanctions and referrals to external agencies such as Police, Social Care etc.

Appendix C

Home Loan Agreement for Issue of College Chrome Book

Please sign, date and return to the College Main Reception. FAO: Mrs Read

Introduction

We are loaning you this laptop for the benefit of your child in supporting and developing their education. With this laptop your child will be able to build on and enhance their skills, knowledge, understanding and complete work remotely, away from College

1. The loan agreement exists between the College and the Named Person who has signed this loan agreement.

Pupil Name: ______________________________

Parent/Carer's Name & Address: ______________________________

____

____

____

2. The laptop will be loaned to the named person for the duration of the period in which the child within their care is on roll at Minsthorpe Community College, including Post 16 if appropriate.

Laptop Serial Number: ______________________________

Laptop Name: ______________________________

When you no longer have a child on roll at Minsthorpe Community College (up to year 11 or Y13) you will have to return the laptop. We will inform you of the dates by when or on which the laptop must be returned.

3. Should you move address from the location you have given us, it is essential that you inform the College at the earliest opportunity.

4. You will be issued with a laptop and power supply. These remain the property of Minsthorpe Community College.

5. You must not install additional software or hardware and at no point must you open the laptop and make changes to the inner hardware.

6. The laptop and the connectivity equipment must not be used for any illegal and/or antisocial purpose.

7. There may be occasions when we need you to return the laptop to College for upgrades and maintenance. Please note that because of these upgrades, it may be necessary to completely remove all information contained on the laptop. Minsthorpe Community College cannot be held responsible for the loss or damage of any data on the laptop during this process. It is your responsibility to return the laptop to College.

During this process, technical members of staff may view data or programmes on the laptop. You will be held responsible to the acceptable use policy at this point. You may want to remove personal data from the laptop before its return.

8. All technical support and maintenance must go through Minsthorpe Community College.

9. If your laptop is stolen you must immediately report it to the police and get a crime reference number. Immediately report this to us; we will make every effort to replace the laptop when we are able.

10. If your laptop is accidentally damaged, immediately contact us. We will do our best to repair the damage, if this is not possible, replacement will be on a case-by-case basis.

<u>Responsibilities you have to care for your laptop</u>

11. You have a responsibility to take reasonable care to ensure the security of the laptop and connectivity equipment.

12. Parents/carers are responsible for the monitoring of appropriate use within the home as the college filtering and monitoring systems will not be activated. This includes access to social media and other age restricted sites.

13. You must not decorate or change the external face of the equipment provided in any way, including affixing stickers.

14. Reasonable health and safety precautions should be taken when using a laptop. The College is not responsible for any damage to person or property resulting from the laptop or equipment loaned.

15. The College is not responsible for any costs resulting from the use of the laptop and the connectivity equipment, including electricity, printer cartridges, paper or any cost occurring from an internet service not provided by the College.

I, the parent/carer, have read or had explained and understand the terms and conditions in the home loan agreement. I understand that by breaching the conditions, the loan of the laptop may be withdrawn by the College.

Signed ________________________________Date __________

Printed Name ____________________________

College Address: Minsthorpe Community College
Minsthorpe Lane
South Elmsall
Pontefract
West Yorkshire
WF9 2UJ

Appendix D
Relevant sections for parent and student reference.

Use of AI

All users of AI will comply with applicable laws, regulations, policies and guidelines governing Keeping Children Safe in Education, intellectual property, copyright, data protection and other relevant areas. There will be no unauthorised use of copyrighted material or creation of content that infringes on the intellectual property of others. We will prioritise the safeguarding of our students and their online safety and will not knowingly use any AI technology that puts their safety or privacy at risk. Staff will not allow or cause intellectual property, including students' work, to be used to train Generative AI models without appropriate consent or exemption to copyright.

We recognise that the technology is rapidly evolving and are committed to remaining at the forefront of developments, adapting our ways of working as necessary. We recognise the leadership in the education sector provided by the Department of Education and the guidance set out in their Statement on Generative Artificial Intelligence in Education. This

Use of AI policy has been informed by that guidance. As guidance and technology changes the policy therefore will need to remain under regular review. This policy will therefore be reviewed annually.

We will be transparent and accountable about the use of AI technology so those stakeholders, including staff, students, parents and other partners understand where and how AI is used and who is responsible. Any stakeholder feedback or questions about the use of AI will be considered and responded to appropriately.

By adhering to this policy, we aim to foster a responsible and inclusive environment for the use of AI in education upholding privacy, fairness, and transparency for the benefit of all involved.

USE OF AI BY STUDENTS

As part of child protection and safeguarding policies and processes, the college will ensure that its student will continue to be protected from harmful content online, including that which may be produced by AI technology and that any AI tools used are assessed for appropriateness for individual student's age and educational needs. We will ensure that staff are aware of the risks of AI which may be used to generate harmful content including deepfake and impersonation materials.

A culture of responsible AI use will be fostered through engaging students in conversations about data privacy, bias, safeguarding, and the social impact of AI applications.

Students will be taught not to enter personal, sensitive or confidential data into generative AI tools including any information that could be used to identify them.

AI tools and technologies may be integrated into teaching and learning activities across various subjects and year groups, providing students with hands-on experience and opportunities to develop AI literacy and skills.

POTENTIAL MISUSE OF AI

Students will receive education on responsible and ethical AI use, including the potential risks and consequences of relying solely on AI tools to complete assignments, coursework, or homework. Students will be encouraged by staff to be clear and transparent about where their work has been created with the assistance of AI.

Teaching staff will emphasise the importance of critical thinking, creativity, and originality in student work, discouraging the misuse of AI as a means of plagiarism or academic dishonesty. Clear guidelines and expectations will be communicated to students regarding plagiarism, ensuring that their work reflects their own efforts and understanding.

The college will follow and adhere to any rules or guidance on the use of AI in assessments given by the Joint Council for Qualifications or individual Exam Board requirements https://www.jcq.org.uk/exams-office/malpractice/artificial-intelligence/ and https://www.jcq.org.uk/examshttps://www.jcq.org.uk/exams-office/blogs/updating-the-jcq-guidance-on-ai-use-in-assessments/office/blogs/updating-the-jcq-guidance-on-ai-use-in-assessments

Teaching staff will employ various assessment methods to evaluate student understanding and ensure that they have genuinely grasped the subject matter. This may include class discussions, oral presentations, practical demonstrations, written reflections, and project-based assessments. By utilizing diverse assessment strategies, teaching staff can verify students' comprehension beyond what AI tools can assess, promoting deep learning and authentic student engagement.

Teaching staff will educate students on the potential misuse of AI by those seeking to deceive or trick students into actions that they would otherwise not contemplate, for example interaction with others who are not who they claim to be but who can imitate who they claim to be using AI technology.

DATA PROTECTION IMPLICATION OF USING AI

Staff and students should be aware that any information entered into a Generative AI model is no longer private or secure. Staff and Students will therefore use Microsoft Co Pilot and other AI tools found in the Microsoft 365 suite. Staff and students must not enter any personal information (personal data, intellectual property or private information (including commercially sensitive information, such as contracts) into any Generative AI model. Staff should make themselves aware of and inform students about the data collection, storage, and usage practices associated with AI technologies, particularly Generative AI.

CYBER SECURITY

Our college will take appropriate measures to guarantee the technical robustness and safe functioning of AI technologies, including:

- Implementing rigorous cybersecurity protocols and access controls through measures such as encryption, security patches and updates, access controls and secure storage.
- Establishing oversight procedures and controls around data practices, system changes, and incident response to maintain integrity.
- Ensuring that any suspected or confirmed security incidents are reported to the IT Services and the Data Protection Officer.
- Maintaining vigilance against material That may be a deepfake (a synthetic media which can be used to create realistic and convincing videos or audio of people saying or doing things they haven't. These can be used to spread misinformation or impersonate someone to commit cyber fraud).
- Training staff and students to be aware of the importance of Cyber Security and the potential involvement of AI to carry out cyber-crime.