Online Safety

Portable use and Internet Related Technologies

Assistant Principal (Safeguarding & Wellbeing) | Autumn 26

Minsthorpe Community College: A place where everyone plays a part in strengthening our learning community through Motivation, Commitment & Care.

This document must be read in conjunction with the College's Polices and relevant DfE Guidance:

- The Safeguarding and Child Protection Policy.
- The Staff Handbook
- The Lone Working Policy
- Anti-bullying Principles and Practice
- Behaviour and Discipline Continuum & Code of Conduct
- Relationship and Sex Education Policy
- The SEND Policy.
- The Offsite Learning Policy

Minsthorpe
Community College

Table of contents

Page

Appendix

Final Section

Section 1

Context

New technologies have become integral to the lives of children and young people in today's society.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

Children and young people should be able to have safe access to the Internet. The College aims to ensure young people are able to use the internet and digital devices appropriately and safely and this is addressed as part of the wider duty of care. Staff have a duty to promote Online Safety through lessons, e.g. using the internet safely and appropriately. The College Online Safety policy should help to ensure safe and appropriate use.

The use of these exciting and innovative tools in College and at home has been shown to raise educational standards and promote student achievement. However, the use of these technologies can put young people at risk within and outside of the College. As indicated in 'Keeping Children Safe in Education' some of the dangers they may face include:

- Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, deepfakes; fake news: misinformation, disinformation & conspiracy theories, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

- Contact: being subjected to harmful online interaction with other users including AI i.e. Chatbots; for example: external 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: online behaviour that increases the likelihood of, or causes, harm; for example, 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 scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/)

It is important to note that this policy is used in conjunction with other College policies (e.g. behaviour, anti-bullying and safeguarding policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to

which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The College must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks without the use of over blocking, making sure that no unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

Section 2

Scope of the policy

This policy applies to all members of the College community (including staff, students, volunteers, parents & carers, visitors, community users) who have access to and are users of College IT systems, both in and out of College.

The Education and Inspections Act 2011 empowers Principals, to such extent as is reasonable, to regulate the behaviour of students when they are off the College site and empowers members of staff to impose sanctions for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Online Safety incidents covered by this policy,

The College will deal with such incidents within this policy and associated Safeguarding, Behaviour and Anti-bullying policies, and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of College

Section 3

Roles and responsibilities

The following section outlines the roles and responsibilities for the Online Safety of individuals and groups within the College. The College is aware of it's responsibilities as outlined in https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges and the roles and responsibilities align and are guided by this documentation. Please refer to Appendix F for further information about the filtering and monitoring processes.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy and Filtering and Monitoring standards. This will be carried out by the Governors receiving regular information about Online Safety incidents and the Governor with a responsibility for Safeguarding is aware of this element within their role.

- Governing bodies and proprietors should support the senior leadership team to make sure effective device monitoring is in place which meets this standard and the risk profile of the school or college.

- Governing bodies and proprietors should support the senior leadership team to review the effectiveness of your monitoring strategies and reporting process.

- Annual monitoring of Online Safety incident logs via the Safeguarding Report to Governors & or Bullying data.

- Termly updates from the AP Safeguarding and wellbeing addressing any current online issues / concerns, following liaison with the Online Safety Lead and DSL

Senior Leaders/Designated Safeguarding Lead

The Principal is responsible for ensuring the safety (including Online Safety) of members of the College community, though the day to day responsibility for Online Safety will be delegated to the IT Services Team leader, Online Safety Lead and DSL, and the Associate Principal Safeguarding and Wellbeing

- The Senior Leaders are responsible for ensuring that staff understand and are appropriately trained to act on reports and concerns which include following all relevant policies and procedures.

- The Senior Leaders are responsible for ensuring that the Associate Team Leader - IT Services, the Online Safety Lead and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant. Ensuring that any safeguarding concerns are acted upon appropriately

- The Senior Leaders will ensure that there are clear system in place to procure and allow for appropriate monitoring and filtering of College systems.

- They will also offer support to those who hold key responsibilities linked to this area in order to review effectiveness of provision. In the main this is monitored by the IT Services Team and AP Student Wellbeing and Safety

- The Designated Safeguarding Lead will monitor suspicious searches or other relevant reports and appropriate action will be taken.

- The Designated Safeguarding Lead will support the Online Safety Team with their responsibilities such as the documentation of decisions pertaining to blocked content, including decision making rationale. Alongside check of filtering and monitoring systems

Online Safety Lead

- Takes day to day responsibility for Online Safety issues which includes the sharing of nudes and semi nudes as set out within UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)

- Has a leading role in establishing and reviewing the College Online Safety policy.
- Takes a lead in Online Safety Education for students.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- Provides training and advice for staff.
- Liaises with College IT technical staff.
- Receives reports of Online Safety incidents via CPOMS (Child Protection Online Management System) and will use this to inform future Online Safety developments and follow up on any incidents logged which may include and liaison with Head of Year, Parent / Carer and students as appropriate.
- Attends relevant meetings.
- Liaise with Designated Safeguarding Lead to inform termly reports to Governors and Senior Leadership.

Associate Team Leader - IT Services

The Associate Team Leader - IT Services is responsible for managing and enforcing the College's network security and filtering.

The Associate Team Leader - IT Services is responsible for ensuring:

- That the College's IT infrastructure is secure and is not open to misuse or malicious attack.
- That users may only access the College's networks through a properly enforced password protection policy.
- That they keep up to date with Online Safety technical information, in order to effectively carry out their Online Safety role and to inform and update others as relevant i.e. by providing filtering and monitoring reports to senior staff; carrying out any checks; actions as necessary.
- That the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Lead, Safeguarding team, Senior Leader, CTL Computing and Digital Media, Class teacher or Head of Year, where appropriate, for investigation, action, support or other sanction.
- That filtering and monitoring software/systems are implemented, maintained and updated as agreed in College policies.
- Application of the following document in co-ordination with Senior Leaders https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges

Teaching and Associate Staff

Teaching and Associate Staff are responsible for ensuring that:

- They have an up to date awareness of Online Safety matters and of the current College Online Safety policy (including Appendices) and practices, and are able to support students when risk assessing online activity.
- They have read, understood and signed the College Staff Acceptable Use (see Appendix A). They are aware that external to College they are responsible for appropriate useage, filtering, monitoring and security of the College owned device.
- They report any suspected misuse or problem to the Online Safety Lead, Safeguarding team, Senior Leader, CTL Computing and Digital Media, Associate Team Leader - IT Services, Class teacher or, Head of Year where appropriate for investigation, action, support or other sanction.
- Digital communications with students (email / student sharepoint / satchel one) should be on a professional level and only carried out using official College systems. Please refer to the Safeguarding Policy for further advice.
- Staff understand and follow the College Online Safety Policy and ensure that the student Acceptable Use (see Appendix B) is being actioned. Where necessary Online Safety information is differentiated appropriately, so that all students, regardless of level of need or ability, fully understand their responsibilities when using IT, to be able to do so safely.
- They monitor IT activity in lessons, extra-curricular and extended College activities and report any concerns including those where systems may have failed to prevent access to inappropriate content I.e. misspelling, abbreviations.
- They are aware of Online Safety issues related to digital devices and they monitor their use and implement current College policies with regard to these devices. If students are seen with a mobile phone staff should confiscate this item and send to hub (refer to mobile phone policy). Refusal to comply will necessitate usual sanction routes.
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use, or where independent research is needed that students are aware of using appropriate sources.
- If staff have reason to suspect that a digital device contains evidence related to an offence which is in breach of law, they must give the device to a member of the Safeguarding Team who will then will then liaise with the police. Any material on the device that is potential evidence, or that may contain child abuse images must not be viewed by staff. The device must be confiscated and switched off without deleting any potential evidence for police.
- If staff members find material that they do not suspect contains evidence in relation to an offence, they can decide whether it is appropriate to ask the student to delete or retain the material as evidence for potential investigation.
- Staff are fully aware of the Keeping Children Safe in Education and have regular training around this area. This policy should be read in conjunction with the College Safeguarding Policy and any other linked policies.

Safeguarding Team (DSLs)

The DSL should be trained in Online Safety issues and be aware of the potential for safeguarding issues to arise from:

- Sharing of personal data.
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Risks associated with AI technology
- Potential or actual incidents of grooming.
- Cyber-bullying.
- Cyber crime

Online Safety Team

Members of the Team will include:
The DSL; Associate Team Leader – IT services; Assistant Principal and other Colleagues responsible for Data Protection to review and ensure appropriate Filtering and Monitoring, cyber security systems are in place.

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.
- 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. 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, Deepfakes, 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.
- Tracking devices i.e. Airtags are not permitted to be used to track children and parent/carers; the College will disable any devices if found.

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.

Community Users

Community Users who access College IT systems will be expected to sign the Acceptable Use see Appendix A

Current Roles of Responsibility

- Assistant Principal Safeguarding and Wellbeing, Designated Safeguarding Lead – Jeanette Collins
- Online Safety Lead and DSL - Amanda Lloyd
- Online Safety Lead – Chris Truelove
- Associate Team Leader - IT Services – Matthew Wood
- CTL Computing and Digital Media – Stuart Mallinson
- Safeguarding Governor – Mrs Bev Semper
- Principal – Mark Gilmore
- Deputy Designated Safeguarding Person – Dale Fairhurst, Georgina Newton & Karen Barker

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 i.e. recognising the harm that misinformation, disinformation can cause.
- 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 including the use of AI refer to Appendix D
- 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.

Staff

It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Annual Safeguarding Training which includes Online Safety.
- All new staff will receive Online Safety within their Safeguarding Induction training and HR issue and ensure that they fully understand the College Online Safety Policy which includes the signing of Appendix A.
- The Online Safety Lead will receive regular updates through their registration for online updates from organisations such as SWGFL and other such corporations.
- The Online Safety Lead will provide advice / guidance / training as required to individuals.

Section 5

Infrastructure / Equipment and Monitoring

The College will be responsible for ensuring that the College infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their Online Safety responsibilities:

- College IT systems will be managed as outlined in Industry Standards.
- There will be termly reviews and audits of the safety and security of College IT systems by the Associate Team Leader - IT Services.
- Servers, wireless systems and cabling will be securely located and physical access restricted.
- All users will have clearly defined access rights to College IT systems. Details of the access rights available to groups of users will be recorded by the IT Services Team leader and will be reviewed, at least annually, by the Online Safety Team.
- All student users will be provided with a username and password by the IT Services Team leader who will keep an up to date record of users and their usernames. Users will be required to keep their passwords secure and will be responsible for all activity using their account.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The College maintains its managed filtering service using Onsite Firewall and filtering system from Fortinet.
- In the event of the IT Services Team leader needing to switch off the filtering for any reason, or for any user, this must be logged.
- Any filtering issues should be reported immediately to the IT Services Team leader or the Online safety Lead or DSL
- Requests from staff for sites to be removed from the filtered list will be considered by the IT Services Team leader and the Online Safety Lead and DSL. Changes will be considered if the educational benefits outweigh risks that could be posed to all stakeholders. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed termly.
- College IT technical staff regularly monitor and record the activity of users on the College IT systems and users are made aware of this in the Appendices.
- Remote management tools are used by staff to control workstations and view users' activity, and this is controlled by net support.
- An appropriate system is in place for users to report any actual / potential Online Safety incident to the IT Services Team leader or the Online Safety Lead and DSL via service desk or CPOMS.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the College systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the College system
- The College infrastructure and individual workstations are protected by up to date virus software.
- Personal data should not be sent over the internet or taken off the College site unless safely encrypted or otherwise secured.
- The college will ensure that any historical, or trending extremist websites, or websites that will promote radicalisation of young people are added to the college blocked site list.

Section 6

Curriculum

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages in the use of IT across the curriculum.

- In lessons where internet use is pre-planned, it is expected that students should be guided to sites checked as suitable for their use and that appropriate procedures are followed for dealing with any unsuitable material that is found in internet searches by reporting to the Online Safety Team.
- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit, and act accordingly should any unsuitable material be accessed.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would normally result in a filtering alert. In such a situation, staff can inform IT Services who can make a request to temporarily remove these sites from the filtered list for the period of study.
- IT Services will inform the Class teacher, DSL and Head of year of any alerts that are not appropriate and accounted for.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information (misinformation, disinformation & conspiracy theories can cause harm). (Staff should seek to reinforce student's ability to risk assess).
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet including the use of AI.

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.
- Staff must ensure that all digital images/video are submitted to the IT Service Desk before publication in any forum.

- 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 as directed by the lead member of staff (see mobile phone policy).
- 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. Measures will be taken to reduce the likelihood of misuse by others i.e. meta data removed; watermarks/banners added etc
- 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 8

Use of Social Media

The College uses a number of systems to allow for communication with students and their families which are closely monitored to ensure all stakeholders are protected e.g. satchel one, College email, College Social Media including twitter and Facebook and a College newsletters. This means that it would be rare for staff to require a different communication platform. If staff require their own Social Media pages they need to have express permission from the Principal and must have signed documentation which is kept with the Director of HR.

All college related social media accounts must be created and implemented following the college guidelines below:

- There must be a clear and demonstrable educational reason for the creation of any college linked social media account.
- Before requesting the creation of an account, approval should be sought from the relevant line manager (following the approval of the Principal), who on agreement, should notify the IT Services team that they have approved the account set-up.
- All accounts must be created by the college's IT Services Team, and appropriate administrator's rights and passwords will be passed to the staff member responsible for the account by the IT Services Team when the account is ready to go live.
- The login and password details may only be changed by the College's IT Services Team.

- All content created must adhere to the guidelines outlined in this policy. Including the use of images see section 7
- If you are blogging, or posting about your work at Minsthorpe Community College, use your real name, identify that you work for Minsthorpe Community College, and be clear about your role.
- Make sure your communication with students or members of the public doesn't violate Minsthorpe Community College privacy or confidentiality and complies with the Colleges' online Safety Policy. All statements must be true and not misleading and all claims must be substantiated and approved. Do not comment on anything unrelated to your subject and the topic the account was created to discuss.
- Make sure you write and post about your areas of expertise, especially as related to Minsthorpe Community College. If you are writing about a topic Minsthorpe Community College is involved with but you are not the Minsthorpe Community College expert on the topic, you should make this clear to your readers. Also respect brand, trademark, copyright, fair use, confidentiality, and financial disclosure laws. If you have any questions about these, see the Associate Team Leader – IT Services for clarification
- What you write is ultimately your responsibility. Please treat your involvement with social media seriously and with respect. In the event of a negative user comment on a social media page which relates to Minsthorpe Community College then it is the responsibility of the page owner/administrator to block, remove or report the post depending on the situation. Use your professional judgement and seek advice from the Associate Team Leader - IT Services or Online Safety Lead and DSL
- Responsibility for the maintenance of a social media page rests with you as the account administrator. If a page is no longer relevant or there is insufficient resource to maintain it, it should be deleted or made non-public.
- If you make a mistake, admit it. Be open and be quick with your correction.
- If you're about to publish something that makes you even the slightest bit uncomfortable, don't shrug it off and hit 'send.' Take a minute to review these guidelines and try to work out what's bothering you, and then alter it. If you're still unsure, you might want to discuss it with your line-manager. Ultimately, what you publish is yours—as is the responsibility.
- In online social networks, the lines between public and private, personal and professional are blurred. Just by identifying yourself as a Minsthorpe Community College employee, you are creating perceptions about your expertise and about Minsthorpe Community College to our students, staff, and the general public.
- Social communication from Minsthorpe Community College should help our students and colleagues. It should be thought-provoking, informative and help to build a sense of community. If it helps people improve knowledge or skills, solve problems, or understand Minsthorpe Community College better — then it's adding value.
- If a page or account's purpose becomes defunct, it is the responsibility of the administrator/owner to delete or deactivate the account.

Section 9

UK GDPR

Any personal data will be held in accordance with UK GDPR which states that the processing of personal data includes:

- Collection
- Organisation
- Structuring
- Storage
- Alteration
- Consultation use
- Communication
- Combination
- Restriction
- Erasure or destruction of personal data.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices. Before sending any outgoing emails that contain sensitive information, please contact the IT Services department for advice on encryption and safe sending. When sending emails that contain attachments these must be password protected ensuring that the password is communicated separately.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The device must be encrypted (including password protection). This can be carried out by the college's IT Support staff on request.
- The data must be securely deleted from the device once it has been transferred or its use is complete.

For further information concerning privacy please visit
https://www.minsthorpe.cc/page/?title=GDPR&pid=134

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 Online Safety Lead and DSL.
- 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 including those generated by AI
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 including those generated by AI
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

Section 12

Responding to Incidents of Misuse

It is expected that all members of the College community will be responsible users of IT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If at any time you become aware, or become concerned that there has been an infringement of our Online Safety policy then you should take action as outlined below:

Keeping students safe online:

- Students must be instructed to use the College Wi-Fi when using their personal devices within College – if permitted by staff to do so.
- If you have any concerns regarding a student's online safety (anything to do with social media, inappropriate use of systems, internet use that causes harm to you, the student or others), please report your concerns via CPOMS in as much detail as possible, as soon as possible. Please do not wait until tomorrow.
- When you log into CPOMS and have clicked 'Add Incident', please ✓Online safety in the "categories" section.
- If a student has any relevant evidence on their personal device, please ask the student to switch the device off (do not delete); confiscate the phone and email classroom assistance giving specific detail about the concerns you have.
- To protect staff we would not advise staff to look at any content on a student phone. If this is needed as part of investigation by Pastoral Leads then students would be asked to share the specific material only. Staff must not view child abuse material even as part of an investigation this includes the sharing of nudes or semi-nudes. If staff have inadvertently viewed 'child sexual abuse material' please speak with a DSL.
- Key Staff will respond to Incidents of youth produced sexual images (nudes/semi nudes) with consultation to the flow diagram in Appendix E.

Keeping yourself safe online:

- Only communicate with students/parents via College systems and insist students to do the same.
- Where possible always use College devices to film/photograph students. If for any reason you need to use your own device (ensure you have permission from the relevant member of leadership), always upload on to the College system and delete at the first opportunity from your own device. When uploading images of students to social media platforms, please check via SIMS that we have photo consent.
- Please be professional online. Please be mindful that you are an employee of Minsthorpe Community College.

- It is essential that you always lock your computer when you leave it unattended and do not keep any student data on your own devices.
- The sharing of College data with outside agencies must be password protected. Passwords should be pre-agreed or telephoned through to the receiving person. To support with the identification of a student initials should only be used.
- We have an online safety section on the college website to support you in staying safe online – https://www.minsthorpe.cc/page/?title=Online+Safety&pid=83 . If you can't find the information you require, then please email Ctruelove@minsthorpe.cc safeguarding@minsthorpe.cc or the IT Service Desk.
- Please remember that "Not everyone is who they seem to be online." This could include our students.

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 A

Acceptable Usage of IT for staff

- I will ensure that I lock my devices if leaving them unattended.
- I will limit the use of mobile devices for personal business within the College to set a strong example to students as indicated in Government guidance.
- I will not access, copy, remove or otherwise alter any other user's files, without their permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the college's policy on the use of digital / video images. Where possible I will not use my personal equipment to record these images. Where these images are published (e.g. on the college website) it will not be possible to identify by name, or other personal information, those who are featured, unless permission has been gained.
- I will only use chat and social networking sites in college in accordance with the College's Online Safety Policy
- I will only communicate with students and parents / carers using official college systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The college has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the college:

- When I use my personal handheld / external devices (PDAs / laptops / mobile phones / USB devices and iPads, etc.) in college, I will follow the rules set out in this agreement, in the same way as if I was using college equipment. I will also follow any additional rules set by the college about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not use personal email addresses on the college IT systems for professional communication.
- Staff are encouraged only to use the College email address for College business and should have their own personal email for other use.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that, where portable storage devices are used, they are encrypted and regularly backed up to the college system.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me

to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in college policies.
- I will not disable or cause any damage to college equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others. Where personal data is transferred outside the secure college network, it must be encrypted.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by college policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for college sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of college:

- I understand that this Acceptable Use Policy applies not only to my work and use of college IT equipment in college, but also applies to my use of college IT systems and equipment out of college and my use of personal equipment in college or in situations related to my employment by the college.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors or dismissal and in the event of illegal activities the involvement of the police.

Use of College equipment

Laptops, iPads, smartphones or other portable devices may be loaned by the College while you are an employee at Minsthorpe Community College to assist in your professional role. These devices remain the property of Minsthorpe Community College. These must be used in line with this document, which will be read and signed by you before equipment is issued. While the equipment is in your care the following points should be noted, as failure to do so

may result in charges being incurred by yourself or disciplinary action being taken against you.

1. Only licenced software should be installed on the equipment. If you intend to use software licenced to yourself, proof of licencing must be provided on request to the IT services team. Use of illegally obtained software is strictly forbidden.

2. Anti-Virus software is installed on the equipment and is updated on a regular basis by automated download when you log on to the College network. You must ensure that you log onto the college network with each device on a regular basis to ensure that software is kept up to date.

3. Should any faults occur with the electronic equipment, then the College's IT Support staff must be advised as soon as possible, so that they may arrange any necessary repairs. Under no circumstances should you attempt to fix suspected hardware faults.

4. A brief training session at the time of issue of any new equipment will give an overview of the equipment and installed software.

5. Any telephone or broadband network charges incurred by accessing the Internet from home while using College equipment are not chargeable to the College.

6. College policies regarding acceptable use, online safety, data protection, computer misuse and health and safety must be adhered to by all users of the equipment.

7. Minsthorpe Community College participates in the Risk Protection Arrangement (RPA) insurance scheme. The cover in respect of the electronic equipment is the same as for any item of equipment in College, that is: -

   I. If the equipment is taken home by a member of staff, then the same cover would apply whilst in the member of staff's home.

8. NB There will be no insurance cover in the following circumstances:

   I. When the equipment is left in an unattended vehicle, unless it is in a locked boot. (If a hatch back it should be concealed under the parcel shelf and must not be on view).
   II. In a parked vehicle overnight, irrespective of whether it is in a locked boot. (The cover will apply if the vehicle is in a locked garage).
   III. There is no cover if the laptop is being conveyed by cycle or motorcycle.

   NB Where a loss of equipment is incurred because of one of these reasons, the replacement cost of the equipment will be billed to the member of staff.

9. If for any reason a claim was made on your home insurance that resulted in the replacement of any college issued equipment, that new equipment would be the property of the College.

10. Details of the make, model, serial number and contents are documented before issue by the IT support team. These will be used as a checklist for returning the equipment as and when your employment at the College ends.

11. If a carry case for the equipment is provided (e.g. a laptop bag) then this MUST be used when transporting the equipment. Failure to comply with this could invalidate any warranty and any damage caused will be billed to the member of staff.

Please now complete the section on the following page to show that you have read, understood and agree to the rules included in the Staff Laptop and Portable Device Acceptable Use Policy.

> I understand that I must use college IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users. I am aware that my use of IT will be monitored whilst on College site and at all other times I need to ensure I am meeting professional standards if using College owned device. I recognise the value of the use of IT for enhancing learning and will ensure that students receive opportunities to gain from the use of IT. I will, where possible, educate the young people in my care in the safe use of IT and embed online safety in my work with young people.

Please sign both of the following statements, then detach and return the bottom copy to Cath Green, Director of HR and Associate Teams. The top copy is your and must be kept safe.

I have read and understand the information within this policy and Appendix A. I accept responsibility for all electronic equipment allocated to me under this initiative and have read and agree to the points above.

Staff, Governor or Visitors Name (Print Name) .....

Signed..... Date.....

✂.....

<u>This copy to be signed and returned to Cath Green, Director of HR and Associate Teams</u>

I have read and understand the information within this policy and Appendix A. I accept responsibility for all electronic equipment allocated to me under this initiative and have read and agree to the points above.

Staff, Governor or Visitors Name (Print Name) .....

Signed..... Date.....

Acceptable Use Statements - to sign and return

This copy to be signed and retained by the member of Staff, Governor and Visitor.

I have read and understand the above and agree to use the college IT systems (both in and out of college) and my own devices (in college and when carrying out communications related to the college) within these guidelines.

Staff, Governor or Visitors Name (Please print) .....

Signed..... Date.....

Please also sign below if the statement is relevant to you:

As a member of the Minsthorpe Community / an ex-student of Minsthorpe Community College, I have contact with students (past / present) / parents of the college in my use of social networking / chat / email / text or instant messaging. I am aware of the need to maintain professionalism in the use of these. I understand that by doing this I could potentially be putting myself at risk and will apply appropriate privacy rights to my accounts to avoid unwanted contact from other students / parents. I accept that this is my responsibility to do this in an attempt to avoid any safeguarding issues that may arise relating to my use of these technologies. If I am unsure of how to apply these privacy rights it is my responsibility to seek advice from the IT Service Team Leader or Online Safety Lead and DSL.

Staff, Governor or Visitors Name (Please print) .....

Signed..... Date.....

This copy to be signed and returned to Cath Green, Personnel and Human Resources Director

I have read and understand the above and agree to use the college IT systems (both in and out of college) and my own devices (in college and when carrying out communications related to the college) within these guidelines.

Staff, Governor or Visitors Name (Please print) .....

Signed..... Date.....

Please also sign below if the statement is relevant to you:

As a member of the Minsthorpe Community / an ex-student of Minsthorpe Community College, I have contact with students (past / present) / parents of the college in my use of social networking / chat / email / text or instant messaging. I am aware of the need to maintain professionalism in the use of these. I understand that by doing this I could potentially be putting myself at risk and will apply appropriate privacy rights to my accounts to avoid unwanted contact from other students / parents. I accept that this is my responsibility to do this in an attempt to avoid any safeguarding issues that may arise relating to my use of these technologies. If I am unsure of how to apply these privacy rights it is my responsibility to seek advice from the IT Service Team Leader or Online Safety Lead and DSL.

Staff, Governor or Visitors Name (Please print) .....

Signed..... Date.....

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 safe 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.

Responsibilities you have to care for your laptop

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

Use of AI

Artificial Intelligence (AI) technology is already widely used in both commercial and everyday applications, and its influence is anticipated to grow exponentially, impacting almost all industries and job sectors including education. Generative AI refers to technology that can be used to create new content based on large volumes of data that models have been trained on from a variety of works and other sources. Generative AI is a rapidly evolving and increasingly freely available technology generating writing, audio, codes, images and video simulations. Whilst this offers opportunities for schools and their students, it also increases risk.

AI is an integral part of the modern world and offers numerous opportunities for enhancing teaching, learning, and administrative processes. This policy establishes guidelines for the responsible and effective use of AI within our college. By embracing AI technology, we aim to:

1. Enhance Learning and Teaching
    - Improve academic outcomes and educational experiences for students.
    - Support teachers in managing their workload more efficiently and effectively.
2. Promote AI Literacy
    - Educate both staff and students about safe, responsible, and ethical AI use.
    - Develop AI skills and understanding as part of digital literacy.
3. Prepare for the Future
    - Equip staff and students for a future where AI is integral to many careers and industries.
4. Support Equity and Inclusion
    - Use AI to address learning gaps and provide personalised support to all learners.
5. Improve College Operations
    - Streamline administrative processes to reduce costs and increase efficiency.
6. Ensure Legal and Ethical Compliance
    - Adhere to laws and regulations related to safeguarding, data protection, copyright, and intellectual property.
    - Avoid using AI in ways that compromise privacy or safety.
7. Maintain Transparency and Accountability
    - Clearly communicate how AI is used in the college and who is responsible for its use.
    - Encourage feedback from stakeholders including staff, students, and parents.
8. Stay Current with Technological Developments
    - Regularly review and update the policy in line with evolving AI technologies and government guidance.

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.

RESPONSIBILITIES

This Policy applies to all staff, including temporary staff, consultants, governors, volunteers, and contractors, and anyone else working on our behalf. It is also applicable to students, but this group will require support and guidance from staff as part of their learning. All staff are responsible for reading and understanding this policy before using any AI technology.

All leaders are responsible for ensuring their staff team read and understand this policy before using AI technology and that they follow this policy, including reporting any suspected breaches of it.

There are a number of staff in the college who are key contributors to this Use of AI policy and its development:

- Matt Wood – Associate Team Leader – IT Services
- Kimberly McGowan – Assistant Principal (AP Assessment & Outcomes / Data Protection Officer)
- Jeanette Collins – Assistant Principal (Student Safety and Wellbeing – DSL)
- Laura Drysdale – Associate Assistant Principal and Quality Nominee
- Chris Truelove – Online Safety Lead
- James Falkiner – Lead Teacher

Training will emphasise how AI can augment staff roles, providing them with more time and resources to focus on tasks such as personalised instruction, student engagement, and critical thinking.

By combining the benefits of AI technology with professionals' expertise, experience, and professional judgment, we can create a collaborative and effective educational environment that maximises the benefits of both human and AI capabilities.

This policy also links to other college policies, including the Safeguarding and Child Protection Policy and Data Protection.

USE OF AI BY STAFF

Staff are permitted to explore and utilise Microsoft Co-pilot and other Microsoft 365 applications that feature AI (AI Tools) to assist in managing their work. Examples of such tasks may include report writing, lesson planning, professional development and facilities management. AI can provide valuable support while still incorporating professional judgment and expertise.

AI Tools will be used responsibly, ensuring they complement staff professional judgment and expertise, without replacing them.

Staff remain professionally responsible and accountable for the quality and content of any output generated by AI, however generated or used.

Staff will receive appropriate training and support to effectively integrate AI into their work including professional development opportunities focused on AI tools and their effective integration into college administrative and teaching practices.

AI Tools can assist staff in gathering and creating relevant educational resources, creating whole group or personalised lesson plans, generating extension tasks or scaffolded work, and identifying potential knowledge gaps. Teaching staff are permitted to use these suggestions as a starting point, incorporating their professional expertise to customise the lesson plans and make necessary adjustments to ensure student learning objectives are met. AI tools can be utilised to automate certain aspects of marking of student work, such as multiple-choice or fill in-the-blank assessments.

Teaching staff can use AI Tools to assist in writing student reports, ensuring accuracy and efficiency while maintaining their professional judgment. Where an AI Tool has been used to support with report writing, the staff member will always review and modify the AI-generated reports to ensure they reflect their own observations, assessments, and personalised feedback.

Staff can use AI as a starting point to gather relevant information and identify patterns in student attainment, but they should rely on their expertise to provide a comprehensive and holistic evaluation of each student's progress. By using AI responsibly in student progress analysis, staff can streamline the process, save time, and ensure consistency. However, they remain the key decision-makers in evaluating and providing feedback on students' academic achievements and overall development.

Where staff use AI as part of their work, they will be clear where it has been used and what additional professional review or revision has been carried out. Staff will not use AI tools or data for personal gain or for any means in contravention of applicable laws.

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. There will be times when students will be clearly told that AI is not to be used for example when produced assessed work.

Teaching staff will emphasise the importance of critical thinking, creativity, and originality in student work. The misuse of AI as a means of plagiarism or academic dishonesty is not acceptable and appropriate sanctions will be put in place if needed. 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.

ETHICAL USE OF AI

The use of AI systems, in particular Generative AI, will be carried out with caution and an awareness of their limitations. Whether staff are using AI for teaching or college administrative purposes, or with students who will make use of this technology, they should be mindful of, and instruct students about, the following considerations:

Bias - data and information generated by AI will reflect any inherent biases in the data set accessed to produce it. This could include content which may be discriminatory based on factors such as race, gender, or socioeconomic background.

Accuracy – information may be inaccurate when generated so any content should be fact-checked.

Currency – some AI models only collate data prior to a certain date so content generated may not reflect the most recent information.

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.

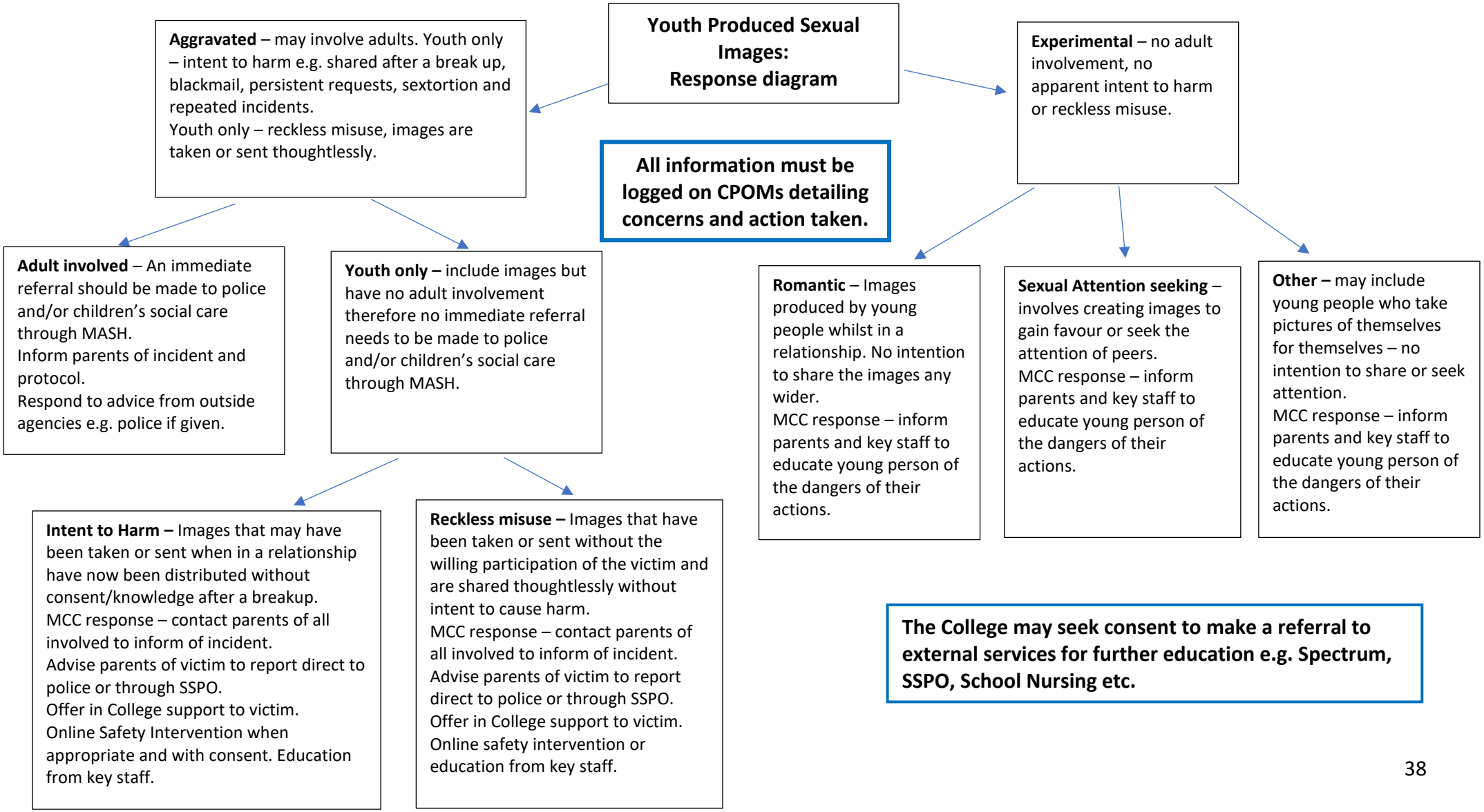
• Ensuring that any suspected or confirmed security incidents are reported to the IT Services and the Data Protection Officer.

• 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.

Appendix E

Managing Incidents of Youth Produced Sexual Images



Appendix F

Filtering and Monitoring

Filtering

DfE Keeping Children Safe in Education requires schools to have "appropriate filtering". DfE published Filtering and monitoring standards for schools and colleges in May 2026
Minsthorpe Community College tests their filtering for protection against illegal materials at: SWGfL Test Filtering
Filtering system are operational, up to date and applied to all:

- users, including guest accounts.
- devices using the school wifi/network connection.

The Fortinet filtering system will:

- filter all internet feeds, including any backup connections.
- be age and ability appropriate for the users and be suitable for educational settings.
- handle multilingual web content, images, common misspellings and abbreviations.
- identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them.
- provide alerts when any web content has been blocked.
- Mobile and App content is filtered by our system and monitored to reduce the risk of harm.

Monitoring

A variety of monitoring strategies are used to minimise safeguarding risks on internet connected devices and may include:

- physical monitoring by staff watching screens of users
- live supervision by staff on a console with device management software (netsupport)
- network monitoring using log files of internet traffic and web access
- individual device monitoring is being explored by the College

Filtering & Monitoring Responsibilities

Please refer to Section 3 of the policy for responsibilities

- Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the Fortinet equipment on site by actively employing the Internet Watch Foundation URL list and other illegal content lists.
- Filter content lists are regularly updated and internet use is logged and frequently monitored.
- The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon including logging safeguarding concerns on CPOMS.
- There is a clear route for reporting and managing changes to the filtering system.
- Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.
- The filtering and monitoring provision is reviewed at least annually and checked regularly.

- There is a defined and agreed process for making changes to the filtering or monitoring system that involves a senior leader in the agreement of the change see section 5

Reviewing the filtering and monitoring provision

The filtering and monitoring provision will be reviewed at least annually. The review will be conducted by the Assistant Principal for student safety and wellbeing (DSL), and the IT manager who liaises with our service providers. Additional checks to filtering and monitoring will be informed by the review process so that governors have assurance that systems are working effectively and that the college is meeting their safeguarding obligations as outlined in KCSIE.

A review of filtering and monitoring will be carried out to identify the current provision, any gaps, and the specific needs of learners and staff.
The review will take account of:

- the risk profile of learners, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what the filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of learners
- teaching requirements, for example, the RHSE and PSHE curriculum
- the specific use of chosen technologies, including Bring Your Own Device (BYOD)
- what related safeguarding or technology policies are in place
- what checks are currently taking place and how resulting actions are handled

To make the filtering and monitoring provision effective, the review will inform:

- related safeguarding or technology policies and procedures
- roles and responsibilities
- training of staff
- curriculum and learning opportunities
- procurement decisions
- how often and what is checked
- monitoring strategies

The review will be carried out as a minimum annually, or when:

- a safeguarding risk is identified
- there is a change in working practice, e.g. remote access or BYOD
- new technology is introduced

Checking the filtering and monitoring systems

Checks to filtering and monitoring systems are completed and recorded as part of the filtering and monitoring review process. How often the checks take place will be based on the context, the risks highlighted in the filtering and monitoring review, and any other risk assessments. Checks will be undertaken from both a safeguarding and IT perspective.

When filtering and monitoring systems are checked this should include further checks to verify that the system setup has not changed or been deactivated. Checks are performed on a range of:

- school owned devices and services, including those used off site
- geographical areas across the site
- user groups, for example, teachers, pupils and guests

Logs of checks are kept so they can be reviewed. These record:

- when the checks took place
- who did the check
- what was tested or checked
- resulting actions

Training

Please refer to previous sections within the policy for further information given to all stakeholders including students and parents i.e. AUP. All staff receive annual safeguarding training and our Online Safety Policy is updated annually in line with the release of KCSIE. Staff briefings and Governor meetings are also utilised as a method for giving regular updates and reminders.
If a serious safeguarding incident were to occur or evidence becomes known of potential failings in the policies and procedures a review would take place sooner.
The DSL and IT Manager have received enhanced training to help them understand the filtering and monitoring systems.

Final Section

Equality Assessment

This policy has been assessed with regard to its impact on equalities issue, with specific reference to the aims of the Equality Act 2010. The equality impact assessment focused on race, gender, disability, pregnancy and maternity, age, sexual orientation, gender identity and religion/belief.

Updates

Sept 26 Section 1 – Content – deepfakes / contact – AI ie Chatbots Section 3 – Teaching and Associate staff – point 7 / Safeguarding team – point 4 / current roles and responsibilities – online safety lead. Section 7 – point 8

Policy Review Schedule

Policy last reviewed:	Due for next review:	Role Responsible:
January 2022	January 2023	Assistant Principal (Safeguarding and Wellbeing)
Summer 2022	Summer 2023	Assistant Principal (Safeguarding and Wellbeing)
Summer 2023	Summer 2024	Assistant Principal (safeguarding and Wellbeing)
Summer 2024	Summer 2025	Assistant Principal (Safeguarding and Wellbeing) Head of Safeguarding
Summer 2025	Summer 2026	Assistant Principal (Safeguarding and Wellbeing) Head of Safeguarding Associate Assistant Principal (Director of Post 16)
Summer 2026	Summer 2027	Assistant Principal (safeguarding and Wellbeing)