Online Safety Policy

Author: Head of IT, MIS & Exams

Equality Assessment: Head of IT, MIS & Exams **Date: August 2025**

Version and Date		Actions/Notes
1.0	August 2024	No changes since last update.
2.0	25/07/2025	Added AI Policy and Data (Use and Access) Act 2025 policy to header sheet Updated Head of IT with Head of IT, MIS & Exams Updated with Cyber Security and AI changes in line with the new Online Safety guidelines provided by 360Safe self-review tool.

Approved by SMT: **August 2025**

Approved by Corporation: **NA**

Date of Next Review: **August 2026**

Related policies or procedures or parent policy if applicable:

Data Breach Policy
Data Protection Policy
Information Security Policy
Staff IT Acceptable Use Policy
Student IT Acceptable Use Policy
IT Security Policy
AI Policy

Groups/bodies consulted in the development of the policy:

Keeping Children Safe in Education 2025
Privacy and Electronic Communications Regulations (PECR)
The Byron Review (2008) and the Byron Progress Review (2010)
What academies, free schools and colleges must or should publish online (DfE, 2016)
Children and Families Act 2014
Equality Act 2010
Protection of Children Act 1978
Protection from Harassment Act 1997
Sexual Offences Act 2003
Public Order Act 1986
Racial and Religious Hatred Act 2006
Criminal Justice & Public Order Act 1994
Copyright, Designs and Patents Act 1988
Regulation of Investigatory Powers Act 2000
The Data Protection Act 2018
Computer Misuse Act 1990
Freedom of Information Act 2000
Communications Act 2003

	Malicious Communications Act 1988 Telecommunications Act 1984 Trade Marks Act 1994 Obscene Publications Act 1959 and 1964 Human Rights Act 1998 The Education and Inspections Act 2011 The Protection of Freedoms Act 2012 Serious Crime Act 2015 Criminal Justice and Courts Act 2015 Data (Use and Access) Act 2025
To be published on College Website:	Yes
To be published on Student Hub:	Yes

Online Safety Policy

1. Purpose

The use of new and emerging technologies in teaching, learning and assessment is paramount to the success of our learners; the College will have to recognise the potential risks associated with this use. The purpose of this policy is therefore to safeguard and protect our learners from risks associated with the use of new and emerging technologies through security measures and training.

2. Scope

This Online Safety Policy outlines the commitment of Macclesfield College to safeguard members of our learning community online in accordance with statutory guidance and best practice.

This policy applies to all members of the college learning community (including staff, students, volunteers, parents and carers, visitors, community users) who have access to and are users of the college digital systems, both in and out of the college. It also applies to the use of personal digital technology on the college campus (where allowed).

The College will deal with such incidents within this policy and associated 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.

3. Responsibilities

To ensure the online safeguarding of members of our learning community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the College.

3.1. Principal and Executive Leadership Team (ELT) are responsible for:

3.1.1. A duty of care for ensuring the safety (including online safety) of members of the learning community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
3.1.2. Be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
3.1.3. Be responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
3.1.4. Ensure that there is a system in place to allow for monitoring and support of those in college who carry out the internal online safety monitoring role.
3.1.5. Receiving regular monitoring reports from the Designated Safeguarding Lead/Online Safety Lead.
3.1.6. Work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

3.2. Governors are responsible for:

3.2.1. The approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

3.2.2. This review will be carried out by the Safeguarding Committee whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

3.2.2.1. Membership of the Safeguarding Committee with the Designated Safeguarding Lead and Head of IT, MIS & Exams.

3.2.2.2. reporting back to relevant governing body meetings.

3.2.2.3. Receiving (at least) basic cyber-security training to enable the governors to check that the College meets the DfE Cyber-Security Standards.

3.2.3. Support the College in encouraging parents/carers and the wider community to become engaged in online safety activities.

3.3. Designated Safety Lead (DSL) will:

3.3.1. Hold the lead responsibility for online safety, within their safeguarding role.

3.3.2. Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.

3.3.3. Meet regularly with the Safeguarding Committee and designated Governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out.

3.3.4. Attend relevant governing body meetings/groups.

3.3.5. Report regularly to the ELT team.

3.3.6. Be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.

3.3.7. Liaise with staff and the Head of IT, MIS & Exams on matters of safety and safeguarding and welfare (including online and digital safety).

3.3.8. Receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments.

3.3.9. Have a leading role in establishing and reviewing the online safety policies/documents.

3.3.10. Promote an awareness of and commitment to online safety education / awareness raising across the college and beyond

3.3.11. Liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated

3.3.12. Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.

3.3.13. Provide (or identify sources of) training and advice for staff/governors/parents/carers/learners.

3.3.14. Liaise with the IT Support team, Safeguarding Officers and support staff (as relevant).

3.3.15. Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education: Content, Contact, Conduct and Commerce.

3.4. Centre Principals will:

3.4.1. Work with the DSL to develop a planned and coordinated online safety education programme.
3.4.2. This will be provided through mapped cross-curricular programme, and tutorial programmes and relevant national initiatives and opportunities (e.g. Safer Internet Day and Anti-bullying week)

3.5. Curriculum and Business Support staff will ensure that:

3.5.1. They have an awareness of current online safety matters/trends and of the current Online Safety Policy and practices.
3.5.2. They understand that online safety is a core part of safeguarding.
3.5.3. They have read, understood, and signed the Staff IT Acceptable Use Policy.
3.5.4. They follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations
3.5.5. All digital communications with learners, parents and carers and others should be on a professional level and only carried out using official school systems and devices (where staff use AI, they should only use college-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements.
3.5.6.
3.5.7. They immediately report any suspected misuse or problem to the DSL for investigation/action, in line with the College's safeguarding procedures.
3.5.8. All digital communications with learners and parents/carers are on a professional level and only carried out using official and trusted College platforms and systems.
3.5.9. Online safety issues are embedded in all aspects of the curriculum and other activities.
3.5.10. Ensure learners understand and follow the Online Safety Policy and Student IT Acceptable Use Policy, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
3.5.11. They supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other college activities (where allowed) and implement current policies regarding these devices.
3.5.12. In lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use and report any unsuitable accessed materials to the IT Support team immediately for investigation.
3.5.13. Where lessons take place using live-streaming or video-conferencing, there is regard to the Remote working agreement.
3.5.14. There is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
3.5.15. They model safe, responsible, and professional online behaviours in their own use of technology, including out of college and in their use of social media.
3.5.16. They adhere to the school's technical security policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity

3.5.17. They have a general understanding of how the learners in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies

3.5.18. They are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

3.5.19.

3.6. Head of IT, MIS & Exams is responsible for ensuring:

3.6.1. They are aware of and follow the Online Safety Policy and IT Security Policy to carry out their work effectively in line with college policy.
3.6.2. The College's technical infrastructure is secure and is not open to misuse or malicious attack.
3.6.3. The College meets the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from other relevant bodies.
3.6.4. There is clear, safe, and managed control of user access to networks and devices.
3.6.5. 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.
3.6.6. The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the DSL for investigation and action.
3.6.7. The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
3.6.8. Monitoring systems are implemented and regularly updated as agreed in college policies.

3.7. **Students**:

3.7.1. Are responsible for using the College's digital technology systems in accordance with the Student IT Acceptable Use Policy and this Online Safety Policy, this includes if they are using their personal devices on the College network.
3.7.2. Should understand the importance of reporting abuse, misuse or access to inappropriate materials to the IT Student Helpdesk.
3.7.3. Should know to report to their tutor or a College Safeguarding Officer if they or someone they know feels vulnerable when using online technology.
3.7.4. Should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.
3.7.5. Should understand the importance of adopting good online safety practice when using digital technologies out of college and realise that the College's Online Safety Policy covers their actions out of college, if related to their enrolment at the College.

3.8. **Parents and carers**:

3.8.1. Play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

3.8.2. The College will take every opportunity to help parents and carers understand these issues through:

3.8.2.1. Publishing the Online Safety Policy on the college website.

3.8.2.2. Seeking their permissions at enrolment concerning use of digital images.

3.8.2.3. Website and social media information about national/local online safety campaigns and literature.

3.8.3. Parents and carers will be encouraged to support the College in:

3.8.3.1. Reinforcing the online safety messages provided to learners in college.

3.8.3.2. The safe and responsible use of their children's personal devices in the College (in areas where this is allowed).

There is an expectation that required professional standards will be applied to online safety as in other aspects of college life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the College and wider community, using officially sanctioned College mechanisms.

4. Safeguarding Committee

The Safeguarding Committee has the following members:

- Designated Safeguarding Lead
- Head of IT, MIS & Exams
- Member of ELT
- Governor
- Centre Principals
- Student Service Lead

Members of the Safeguarding Committee assist the DSL and Head of IT, MIS & Exams with:

- The review of the Online Safety Policy/documents.
- The review and monitoring of the college filtering policy and requests for filtering changes
- Mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage.
- Reviewing network/filtering/monitoring/incident logs, where possible.

5. Objectives

Our Online Safety Policy:

- Sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication.
- Allocates responsibilities for the delivery of the policy.
- Is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours.
- Establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the college and how they should use this understanding to help safeguard learners in the digital world.
- Describes how the college will help prepare learners to be safe and responsible users of online technologies.
- Establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- Is supplemented by a series of related acceptable use agreements.
- Is made available to staff at induction and through the Staff Intranet
- Is published on the college website.

6. Acceptable use

The College has defined what it regards as acceptable/unacceptable use, and this is shown in the tables below.

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to college networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
	• Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) Serious or repeat offences will be reported to the police.					
Users shall not undertake activities that are not illegal but are classed as unacceptable in college policies:	Accessing inappropriate material/activities online in a college setting including pornography, gambling, drugs. (Informed by the college's filtering practices and AUPs)			X	X	
	Promotion of any kind of discrimination				X	
	Using College systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the College				X	
	Infringing copyright and intellectual property (including through the use of AI services)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the College or brings the College into disrepute				X	

Consideration should be given for the following activities when undertaken for non-educational purposes:	Staff				Students			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected courses	Not allowed	Allowed	Allowed at certain times	Allowed for relevant courses
Online gaming								
Online shopping/commerce								
File sharing								
Social media								
Messaging/chat								
Entertainment streaming e.g. Netflix, Disney+								
Use of video broadcasting, e.g. YouTube, Twitch, TikTok								
Mobile phones may be brought to college								
Use of mobile phones for learning at college								
Use of mobile phones in social time at college								

Taking photos on non-College managed mobile phones/cameras								
Use of other personal devices, e.g. tablets, gaming devices								
Use of personal e-mail for college data, or on the college network/wi-fi								
Use of College e-mail for personal e-mails								
Cryptocurrency Mining								
Use of AI services that have not been approved by the college								

The Online Safety Policy and IT Acceptable Use Policies define acceptable use at the College. The acceptable use agreements will be communicated/re-enforced through:

- Student Online Portal
- Student Induction
- Splash Screens whilst accessing online platforms
- Digital Signage
- Posters and notices where technology is used.
- Built into tutorial and education sessions.
- College website

When using communication technologies, the College considers the following as good practice:

- When communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned, auditable, secure and trusted by the College.
- Any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. *Personal e-mail addresses, text messaging or social media must not be used for these communications.*
- Staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the College and its community.
- Users should immediately report to their tutor or a Safeguarding Officer - the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Relevant policies and permissions should be followed when posting information online e.g., college website and social media. Only College e-mail addresses should be used to identify members of staff and learners.

7. Reporting and Responding

The College will take all reasonable precautions to ensure online safety for all College users but recognises that incidents may occur inside and outside of the College (with impact on the College) which will need intervention. The College will ensure:

- There are clear reporting routes which are understood and followed by all members of the learning community which are consistent with the college safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- All members of the learning community will be made aware of the need to report online safety issues/incidents.
- Reports will be dealt with as soon as is practically possible once they are received.
- The DSL, Head of IT, MIS & Examsand other responsible staff have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed safeguarding procedures, this may include:

    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy

- Any concern about staff misuse will be reported to Human Resources.
- Where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss.
- Where there is no suspected illegal activity, devices may be checked using the following procedures:

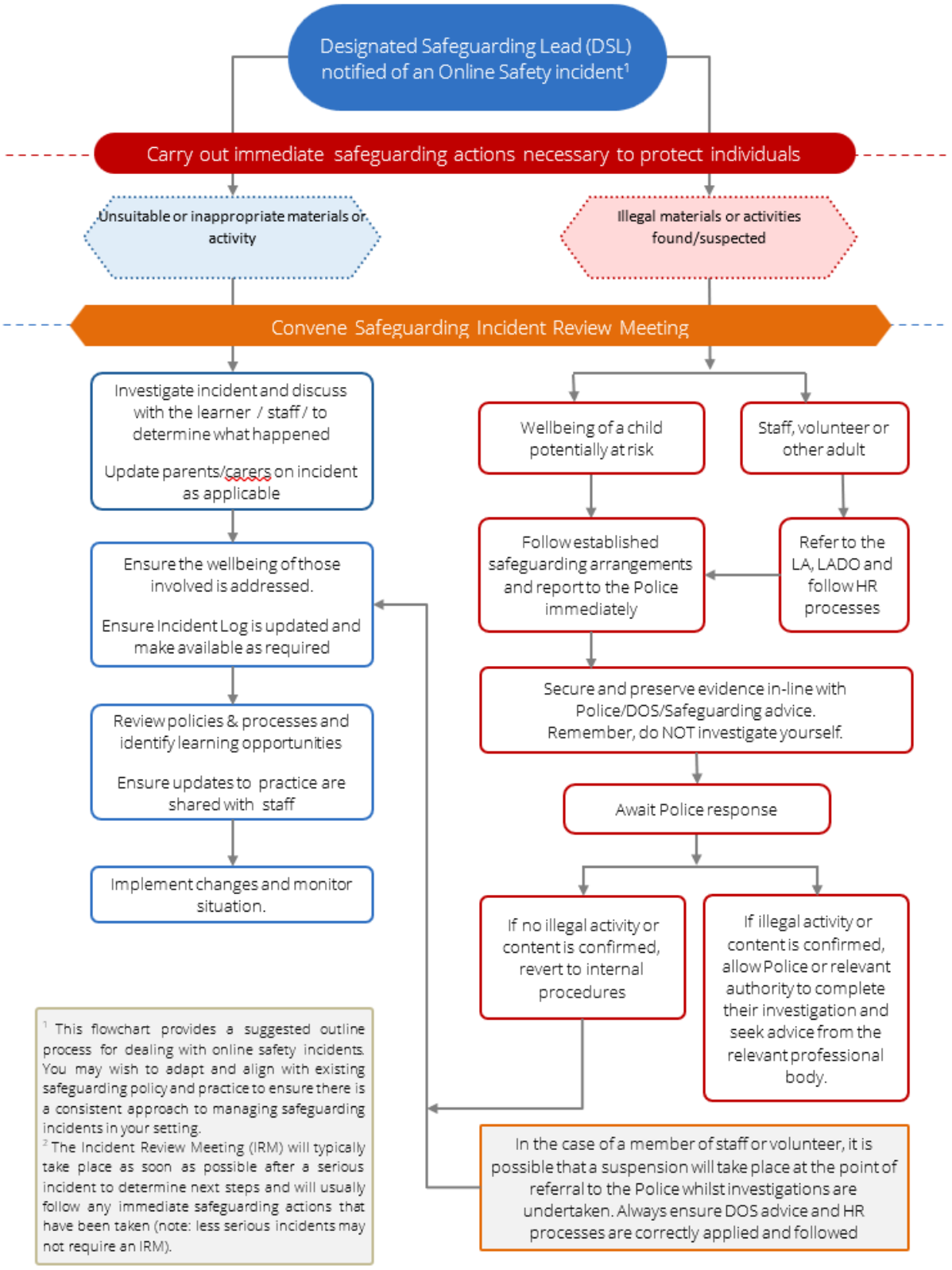
    - One or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - Conduct the procedure using a designated device that will not be used by students and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form.

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- involvement by local authorities (as relevant)
- police involvement and/or action

- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.
- There are support strategies in place e.g., peer support for those reporting or affected by an online safety incident.
- Incidents should be logged by the DSL on the information management system.
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police.
- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions.
- Learning from the incident (or pattern of incidents) will be provided to:

    - The Safeguarding Committee for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
    - Staff, through regular staff briefings
    - Learners, through tutorials/classes
    - Parents/carers, through newsletters, social media, website
    - Governors, through regular safeguarding updates
    - Local authority/external agencies

The College will follow the flowchart below to support the decision-making process for dealing with online safety incidents. Refer to **Appendix 1** to support this process.



It is more likely that the College will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the College community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

7.1. Responding to Learner Actions

Incidents	Refer to class tutor	Refer to Centre Principal	Refer to Principal	Refer to Safeguarding Team	Refer to Police/Social Work	Refer to trusted IT Partners	Inform parents/carers	Remove device/ network/internet access	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).	X	X	X	X	X			X	X	X
Attempting to access or accessing the college network, using another user's account (staff or learner) or allowing others to access college network by sharing username and passwords	X	X						X	X	X
Corrupting or destroying the data of other users.		X				X		X	X	X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X		X				X	X	X

Unauthorised downloading or uploading of files or use of file sharing.	X	X						X	X	X
Using proxy sites or other means to subvert the college's filtering system.	X	X		X				X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident.				X					X	
Deliberately accessing or trying to access offensive or pornographic material.				X				X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	X	X						X	X	X
Unauthorised use of digital devices (including taking images)	X	X		X				X	X	X
Unauthorised use of online services	X	X		X				X	X	X
Actions which could bring the college into disrepute or breach the integrity or the ethos of the College.	X	X	X				X	X	X	X
Continued infringements of the above, following previous warnings or sanctions.		X	X	X			X	X	X	X

7.2. Responding to Staff Actions

Incidents	Refer to line manager	Refer to Principal	Refer to HR \ Safeguarding	Refer to Police	Refer to trusted IT partner	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X	X	X		X	X	X
Actions which breach data protection or network / cyber-security rules.	X		X			X	X	X
Deliberately accessing or trying to access offensive or pornographic material			X				X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X				X	X	X	X
Using proxy sites or other means to subvert the college's filtering system.	X		X			X	X	X
Unauthorised downloading or uploading of files or file sharing	X		X			X	X	X
Breaching copyright/ intellectual property or licensing regulations (including through the use of AI systems).	X					X	X	X
Allowing others to access college network by sharing username and passwords or attempting to access or accessing the college network, using another person's account.	X		X		X	X	X	X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X		X			X	X	X

Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers	X		X			X		
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	X		X			X		
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X		X			X		X
Actions which could compromise the staff member's professional standing	X		X			X	X	X
Actions which could bring the college into disrepute or breach the integrity or the ethos of the college.	X	X	X			X	X	X
Failing to report incidents whether caused by deliberate or accidental actions	X		X			X		
Continued infringements of the above, following previous warnings or sanctions.	X	X	X				X	X

8. Artificial Intelligence (AI) systems in College

Please refer to the College AI Policy for more information.

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in colleges: learner support, teacher support and college operations; ensuring all use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.
The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

The college acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.

We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK Data Protection laws.

We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.

We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.

As set out in the acceptable use policies, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information. Staff will always ensure AI tools used comply with data protection regulations. They must verify that tools meet data security standards before using them for work related to the college. Only those AI technologies approved by the college may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.

We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.

The college will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.

AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.

The college will audit all AI systems in use and assess their potential impact on staff, learners and the college's systems and procedures through Data Protection Impact Assessments for new systems. We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.

AI tools may be used to assist teachers in the assessment of learners' work, identification of areas for improvement and the provision of feedback. Teachers may also support learners to gain feedback on their own work using AI.

Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.

We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.

Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action.

9. Training Programme

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities.

Students will be able to give feedback and their opinions of online safety through the regular Student Voice meetings.

Staff and Governors take part in Online Safety and Data Protection training at induction and also throughout the year.

10. Technology

The College is responsible for ensuring that the infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The college should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

10.1. Filtering & Monitoring

The College filtering and monitoring provision is agreed by the Designated Safeguarding Lead, the Safeguarding Committee and the IT Support team and is regularly reviewed (in August each year or post-incident) in a documented and structured process and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both Safeguarding and IT Support to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT Support team will have technical responsibility.

Weekly checks on the filtering and monitoring system alerts are carried out by the IT Support team.

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole college approach to online safety empowers a college to protect and educate students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

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

- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** 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.
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Online safety and the college's approach to it is reflected in this policy, amongst other things, includes appropriate filtering and monitoring on college devices and the college networks. Considering the 4Cs (above) will provide the basis of an effective online policy.

The college allows the use of mobile and smart technology due to the age range of students, but phones are expected to be away and on silent during class time and also during exam/assessment time according to the Examination rules. Personal devices usually have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 4G and 5G) and this access means some students could by exposed in inappropriate / harmful content. The college will educate the on the safe use of technology and also the acceptable use policies and the rules around appropriate use (See section 6) will still be applied when staff and students are using personal devices in college or for college work. Disciplinary actions will take place for personal device infringements as they would on college-owned devices.

Filtering

The College manages access to content across its systems for all users and on all devices using the College's web filtering solution. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.

Illegal content (e.g., child sexual abuse images) is filtered by filtering solution Content lists are regularly updated.

There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures.

Users can request to unblock or report inappropriate content to the IT Helpdesks, recognising that no system can be 100% effective.

Filtering logs are regularly reviewed and alerted to Designated Safeguarding Lead and relevant Centre Principal to breaches of the filtering policy, which are then acted upon.

There are regular checks of the effectiveness of the filtering systems. Checks are undertaken across a range of devices at least termly and the

results recorded and analysed to inform and improve provision. The DSL is involved in the process and aware of the findings.

Devices that are provided by the college have college-based filtering applied irrespective of their location.

The College has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages/times and different groups of users: staff/learners, etc.).

The College BYOD / guest network is also subject to filtering policies.

Monitoring

The College has monitoring systems in place agreed by the IT Support team and DSL to protect the college, systems and users:

- The College monitors all network use across all its devices and services.
- Monitoring reports are urgently picked up, acted on and outcomes are recorded, and all users are aware that the network (and devices) are monitored at point of access.
- There are effective protocols in place to report abuse/misuse through the IT Helpdesks. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review is conducted by the designated safeguarding lead and technical staff and fed back to the Safeguarding Committee whjch includes the responsible governor. The results of the review will be recorded and reported as relevant.

The College follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and systems through the use of the appropriate blend of strategies informed by the College's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the college of breaches to the filtering policy, allowing effective intervention.

Responsibilities around Filtering and Monitoring

Identified and assign roles and responsibilities to manage out filtering and monitoring systems include:

Role	Responsibility

Safeguarding Committee Lead Governor Information Security Committee Lead Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met. Our Governing Body will ensure online safety is a running and interrelated theme whilst devising and implementing their whole college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.
ELT Team	Responsible for ensuring these standards are met and: • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports Ensure that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns
Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which could include overseeing and acting on: • filtering and monitoring reports • safeguarding concerns • checks to filtering and monitoring systems
Head of IT, MIS & Exams	Technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems
All staff	All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if: • they witness or suspect unsuitable material has been accessed • they can access unsuitable material • they are teaching topics which could create unusual activity on the filtering logs • there is failure in the software or abuse of the system • there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks • they notice abbreviations or misspellings that allow access to restricted material

11. Security

The College IT systems will be managed in ways that ensure that they meet the requirements of the following relevant College policies:

- IT Security Policy
- Data Protection Policy
- Information Security Policy
- AI Policy

12. Mobile Technologies

The IT Acceptable Use Policies for Staff and Students outline the expectations around the use of mobile technologies.

The College allows the following in terms of device access to the network:

	College devices		**Personal devices**		
	College owned for individual use	College owned for multiple users	Student owned	Staff owned	Visitor owned
Allowed in College	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	No	No	No
Internet only	No	No	Yes	Yes	Yes

12.1. College owned/provided devices

All College devices are managed though the use of Mobile Device Management software

There is an asset log that clearly states whom a device has been allocated to.

Personal use (e.g. online banking, shopping, images etc.) on college owned devices is clearly defined and expectations are well-communicated.

Signed loan agreements are in place for liability for damage, return/replacement of equipment and responsible use.

12.2. Personal devices

Use of personal devices are segregated effectively from college owned systems and data.

The expectations for taking/storing/using images/video aligns with the College's acceptable use policy and Social Media policy. The non-consensual taking/using of images of others is not permitted.

Liability for loss/damage or malfunction of personal devices is with the owner of that device.

Staff and students are encouraged to keep their personal devices up-to-date with the latest security updates to ensure they are safe online.

13. Social Media

The College provides the measures in the College's IT Acceptable Use Policies to ensure reasonable steps are in place to minimise risk of harm to learners on social media platforms.

14. Online Publishing, Images and Video

The College will inform and educate staff and students about the risks of publishing photos and videos online.

- The College may use live-streaming or video-conferencing services in line with remote working/learning and safeguarding guidance / policies.
- When using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- Staff/volunteers must be aware of those learners whose images must not be taken/published.
- Those images should only be taken on college owned devices. The personal devices of staff should not be used for such purposes.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at college events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims on college owned devices, but must follow college policies concerning the sharing, storage, distribution and publication of those images.
- Care should be taken when sharing digital/video images that learners are appropriately dressed.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the College website, or elsewhere that include students will be selected carefully and will comply with this Online Safety Policy.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Permission will be obtained during enrolment before photographs of students are taken for use in college or published on the College website/social media. Permission is not required for images taken solely for internal purposes.
- Parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the Data Protection and Retention policy.
- Student work can only be published with the permission of the student.

The College website is managed/hosted by LDA. The College Marketing team ensures that this Online Safety Policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of calendars and personal information - ensuring that there is least risk to members of the learning community, through such publications.

15. Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation. Please refer to the College's Data Protection Policy for more information.

The college ensures that where AI services are used, data privacy is prioritised.

16. Cyber Security

The college has reviewed the DfE Cyber security standards for schools and colleges and continues to work toward meeting these standards.

The college conducts cyber risk audits and has achieved Cyber Essentials Certification.

The college (in partnership with their technology support partner Jisc), has identified the most critical parts of the school's digital and technology services and sought assurance about their cyber security.

The college has an effective backup and restoration plan in place in the event of cyber-attacks.

The college's governance and IT policies reflect the importance of good cyber security.

Staff and Governors receive training on the common cyber security threats and incidents that colleges experience.

The college's education programmes include cyber awareness for learners at induction.

The college has a business continuity and incident management plan in place.

There are processes in place for the reporting of cyber incidents and phishing emails.

All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this and feel safe and comfortable to do so.

17. Review and Monitoring

The relevance, efficacy and effectiveness of this Online Safety Policy will be reviewed in line with the cycle of strategic management activities to facilitate continuous improvement. The results of the review process will be analysed and changes made to the policy where appropriate.

The Head of IT, MIS & Exams and Designated Safeguarding Lead as well as key members of staff make up the Safeguarding Committee. The impact of the policy will be reviewed at this committee and monitored regularly as any incidents occur.

Appendix 1: Record of reviewing devices/internet sites (responding to incidents of misuse)

Group/Course: .....

Date: .....

Reason for investigation: .....

.....

.....

.....

Details of first reviewing person

Name: .....

Position: .....

Signature: .....

Details of second reviewing person

Name: .....

Position: .....

Signature: .....

Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address/device	Reason for concern
Conclusion and Action proposed or taken	