Myerscough College
Opportunities for all to succeed

Staying Safe Online and Use of Mobile Technology Policy and Procedure

This policy is part of the College's Statutory Safeguarding/Learner Protection and Prevent Policy. Any issues and concerns with online safety must follow the College's safeguarding and child protection processes.

The purpose of this policy is to:

- Set out the key principles expected standards in relation to IT at Myerscough College with respect to the use of IT-based technologies and equipment.
- Safeguard and protect the students and staff in relation to unacceptable behaviours, e.g. online safety, grooming, extremism and radicalisation
- Assist College staff working with students to work safely and responsibly with the Internet and other IT and communication technologies and to monitor standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to the responsible use of the Internet for educational, personal or recreational use for the whole college.
- Have clear structures to deal with referrals of online abuse such as bullying
- Ensure that all members of the College community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Follow Safeguarding / IT guidelines to prevent issues in relation to students and staff.

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

1. Introduction and Overview

2.

The main areas of risk for our College community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Confirmation and validation of access to appropriate online resources

Contact

Inappropriate online contact including:

- Grooming, sexual exploitation, radicalisation, extremism etc.
- Online bullying in any form
- Social or commercial identity theft, including passwords etc.

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Coercing

plus, many others.

Roles and Responsibilities

Role	Key Responsibilities
Principalship and Senior Leadership Team	• Must be adequately trained in safeguarding and prevent, in line with statutory guidance and relevant legislation; including KCSIE 2016 and Counter Terrorism Security Awareness 2015 (Prevent legislation) • To promote a 'safeguarding' culture, ensuring that online safety is fully integrated with whole College • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security ensuring College's provision follows best practice in all areas including information handling • To ensure the College uses appropriate IT systems and services • To be responsible for ensuring that all staff receive suitable training to carry out their roles

Role	Key Responsibilities
	• To be aware of procedures to be followed in the event of a serious online safety incident • Ensure suitable risk assessments are undertaken so the curriculum meets the needs of students, including promotion of fundamental British and College Values • Ensure curriculum and tutorial resources include information and guidance to prevent risk of students being radicalised or subject to extremism or any form of grooming • To regularly monitor and review related policies and procedures • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. IT staff • To ensure Governors are regularly updated on the nature and effectiveness of the College's arrangements for safeguarding and Prevent • To ensure the College website includes relevant information for the community
Designated Senior Lead (DSL) Designated Senior Persons (DSPs)	• Take day to day responsibility for online safety issues. The DSP Safeguarding and Prevent Steering Group will review the College's online safety policy/documents and related practice • Promote an awareness and commitment to online safety throughout the College community • Ensure that British Values and online safety education is promoted and embedded within the curriculum • DSL meets Safeguarding / Prevent Governor on a regular basis and reports on related areas of activity. DSL reports to Principalship on a monthly basis. Director of IT and MIS meets Deputy Principal - Resources on a weekly basis • To ensure that all staff are aware of the procedures that need to be followed in the event of any online safety disclosure • To ensure that online incidents are recorded and actioned on the Student Support Register (SSR) • Co-ordinate related training and ensure CPD records are updated • Provide advice for all staff and students • Ensure student surveys / student feedback includes online safety issues and an awareness of Prevent • Liaise with the Local Authority and relevant agencies • DSPs are regularly updated in online safety issues and legislation, and are aware of the potential for serious child protection concerns
Governors / Safeguarding & Prevent Governor	• To be informed that the College has in place policies and practices to keep students and staff safe online • To support the DSL / DSPs • The role of the Safeguarding / Prevent Governor will include regular review meetings with the DSL

Role	Key Responsibilities
Curriculum Managers Meeting	• To oversee the embedding and delivery of the online safety element into the curriculum e.g. My Safety and My Wellbeing • To support promotion and embedding of fundamental British Values
IT Support	• To report online safety related issues that come to their attention, to the Designated Senior Person • To manage the College's computer systems, ensuring: - College password process is strictly adhered to - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls exist to protect personal and sensitive information held on College devices - the College's process on web filtering is applied and updated on a regular basis • Awareness of the College's IT policy, procedures and technical information in order to effectively carry out their role and to inform and update others of any related concerns • That the use of College technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the DSP's • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the College's online security and technical procedures
Business Support and Data Teams	• To ensure that the data they manage is accurate and up-to-date • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements • The College must be registered with Information Commissioner
Teaching Staff	• To embed online safety in the curriculum and promote British Values • To ensure that students are fully aware of their responsibilities including using research appropriately relating to electronic content such as copyright laws
All Staff, Volunteers and Contractors	• To read, understand, sign and adhere to the College Staff Acceptable Use Policy, and understand any updates annually. The AUP is signed by new staff on induction • To report any suspected misuse or problem to the Designated Senior Person (DSP) • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology **Staff Leavers:** • At the end of the period of employment/volunteering to return any equipment or devices loaned by the College. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and Desktop Support Team as required

Role	Key Responsibilities
Students	• Read, understand, sign and adhere to the Student Acceptable Use Policy annually • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe be haviours and good online safety practice when using digital technologies out of College and realise that the College's Online Safety Policy covers their actions online at any location • To contribute to any Learner Voice survey that gathers information of their online experiences
Parents/Carers	• To have an awareness that the College manages online and IT resources and developments to ensure learners stay safe • To consult with the College if they have any concerns about any learners use of technology • To support the College in promoting online safety and endorse the Acceptable Use Agreement which includes the learners' use of the internet and the College's use of photographic and video images

Communication:

The policy will be communicated to staff/students/community in the following ways:

- Via the College intranet
- Via the Child Protection and Safeguarding Policy and Procedure on the website and intranet
- Policy to be referenced during induction for new staff
- Regular updates and training on online safety for all staff, including Safeguarding refresher
- Acceptable Use Policy discussed with staff and students at the start of each academic year. Acceptable Use Policy to be made available to the whole student community during timetabled IT inductions

Handling Incidents:

- The College will take all reasonable precautions to ensure online safety
- Staff and students are given information about expectations, IT acceptable use and related consequences including discipline where appropriate
- Designated Senior Person (DSP) acts as first point of contact for any incident
- Any suspected online risk or infringement is reported to DSP as soon as possible following reporting systems
- Any concern about staff misuse is always referred directly to the Designated Senior Person, unless the concern is about a DSP, in which case the complaint is referred to the Principal/Safeguarding Governor

Review and Monitoring

The Online Safety Policy is referenced within other College policies.

The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the College or new legislation.

The policy will be promoted accordingly and reviewed by the Safeguarding and Prevent Steering Group. All amendments to the College Online Safety Policy and Procedure will be disseminated to all members of staff and students.

2. Education and Curriculum

Student Online Safety Curriculum

The College:

- Has a clear, progressive online safety education programme embedded as part of the curriculum. This covers a range of skills and behaviours appropriate to student age and experience
- Will remind students about their responsibilities through the Student Acceptable Use Policy
- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright - inside and outside of the College
- Ensures that staff and students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights

Staff and Governor Training

This College:

- Makes regular training available to staff on online safety and provides regular advice
- As part of the induction process, all new staff, including volunteers and those on work experience have IT information and guidelines explained

Parent/Carer Awareness and Training

This College:

- Provides information for parents/carers which includes online safety

3. Expected Conduct and Incident Management

Expected Conduct

In this College, all users:

- Are responsible for using the College IT and communication systems in accordance with the relevant Acceptable Use Policy
- Understand the significance of misuse or access to inappropriate materials and are aware of the consequences
- Understand it is essential to reporting any form of abuse, misuse or access to inappropriate materials and know how to do so
- Understand the importance of adopting good online safety practice when using digital technologies in and out of College
- Know and understand College policies on the use of mobile and hand held devices including cameras, tablets (iPads and other related equipment) and mobile phones

Staff, Volunteers and Contractors

- Know to be vigilant in the supervision of students at all times, as far as is reasonable, and use common-sense strategies in learning resource areas where older students have more flexible access
- Know to take professional, reasonable precautions when working with students, previewing websites before use; using age-appropriate search engines where more open Internet searching is required with vulnerable individuals

Parents/Carers

- Should know and understand that the College has rules and guidelines for the appropriate use of IT and will take appropriate action when required

Incident Management

In this College:

- There is strict monitoring and application of the online safety policy and action will be taken as necessary. All members of the College are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the College's processes
- Support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police) in dealing with online safety issues
- Monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in online safety within the College
- Parents/Carers are specifically informed of online safety incidents involving young people when appropriate
- The Police will be contacted if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform other appropriate authorities including Channel as necessary

4. Managing IT and Communication System

Internet Access, Security (Virus Protection) and Filtering

This College:

- Informs all users that Internet/email use is monitored
- Has the educational filtered secure broadband connectivity through JaNet
- Adopts JaNet AUPs and ISP filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gambling)
- Ensures network health is monitored through use of anti-virus software
- Enforces local web filtering through the Firewall. Any changes to the filtering policy are logged and only approved by staff with the appropriate status
- Works in partnership with appropriate authorities to ensure any concerns about the systems are communicated so that procedures remain robust and protect students and staff

Network Management (User Access, Backup)

This College:

- Uses individual, audited log-ins for all users
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Uses 'remote' management access tools for anonymous control of workstations / viewing users / setting-up applications and internet web sites, where appropriate
- Has additional local network monitoring and auditing software installed
- Ensures the network management team is up-to-date with patch management and security policies
- Has an agreed schedule for the back-up of College data
- Storage of all data within the College will conform to the EU and UK data protection requirements; storage of data online, will conform to the EU data protection directive where storage is hosted within the EU

To ensure the network is used safely, this College:

- Ensures staff read the College's Staying Safe Online and Use of Mobile Technology Policy and Procedure. Following this, they are set-up with internet, email access and network access. Online access to service is through a unique, audited username and password. The same credentials are used to access the College's network
- All students have their own unique username and password which gives them access to the internet and other services;
- Makes clear that no one should log on as another user and makes clear that students should never be allowed to log-on or use teacher and staff logins
- Staff and students are expected to save work on their M365 OneDrive and access files and data from these areas
- Requires all users to log off when they have finished working or are leaving the computer unattended
- Ensures all equipment owned by the College and/or connected to the network has up to date virus protection

- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the College, is used primarily to support their professional responsibilities
- Maintains equipment to ensure Health and Safety is followed
- Ensures that access to the College's network resources from remote locations by staff is audited and restricted and access is only through College approved systems
- Does not allow any outside agencies to access our network remotely, except where there is a clear professional need, and then access is audited restricted and is only through approved systems
- Has a clear disaster recovery system in place that includes a secure, remote back up of data
- The wireless network is secured to industry standard enterprise security level, suitable for educational use;
- All IT and communications systems are installed professionally and regularly reviewed to ensure they meet health and safety standards

Password Policy

- This College makes it clear that staff and students must always keep their passwords private, must not share with others; If a password is compromised the IT Department should be notified immediately
- All staff have their own unique username and private passwords to access College systems. Staff are responsible for keeping their password(s) private
- We require staff to change their passwords every 90 days

Email

This College:

- Provides staff with an email account for their professional use
- Will contact the Police if one of our staff or students receives an email that we consider is particularly disturbing or breaks the law
- Will ensure that email accounts are maintained and up to date
- Uses a number of technologies to help protect users and systems in the College, including end user device anti-virus products, email filtering and sandbox detection for malware

Students

- Students are taught about the online safety and how to access on line systems both in College and at home.

Staff

- Staff will use College on line systems for professional purposes only
- Staff will never use email to transfer staff or student personal data outside of the network. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption

College Website

- The Strategic Planning Group, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The College website complies with statutory requirements
- The majority of the website content is the College's own work; where other sites are published or linked to, we credit the sources used and state clearly the author's identity or status

Cloud Environments

- Uploading of information onto the College's online learning space is shared between different staff members according to their responsibilities
- Photographs and videos uploaded onto the College's online environment will only be accessible by members of the College community
- In College, students are only able to upload and publish within College approved 'Cloud' systems

Social Networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate
- Staff are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the College's preferred system for such communications
- For the use of any College approved social networking, will adhere to College's Social Media Policy and Procedure

College staff will ensure that in private use:

- No reference should be made in social media to students, parents/carers or College staff
- They should not become online friends with any student under the age of 18 or vulnerable; any exceptions must be approved by a DSP
- They do not engage in online discussion on personal matters relating to members of the College community or College business
- Personal opinions should not be attributed to the College or compromise the professional role of the staff member, nor bring the College into disrepute
- Personal social media profiles are regularly checked to minimise risk of loss of personal information any issue brought to the College's attention will be followed up and actioned accordingly

Students:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through The Core
- Students are required follow Myerscough College's Acceptable Use Policy

Parents:

- Parents are reminded about social networking risks and protocols through our parental communication and with additional materials when required.

CCTV

- We have CCTV in the College as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted. We will not reveal any recordings without appropriate permission
- We use specialist lesson recording equipment on occasions as a facility to share best teaching practice. We do not reveal any such recordings outside of the college environment unless approval has been given

5. Data Security: Management Information System Access and Data Transfer

Strategic and Operational Practices

At this College:

- The Director of Corporate Services is the Senior Information Risk Officer (SIRO)
- We ensure that staff know how to report any incidents where data protection may have been compromised or to raise safeguarding or prevent concerns
- All staff are DBS checked and records are held in a single central record with annual updating of staff records

Technical Solutions

- Staff have allocated space on OneDrive and / or SharePoint to store their files and data
- All data stored in SharePoint and OneDrive is encrypted by default
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time
- All servers are in lockable, secure locations and managed by IT/ DBS-checked staff
- Details of all College-owned hardware is recorded in a hardware inventory
- Details of all College-owned software are recorded in a software inventory
- Disposal of all equipment in scope will conform to The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007, updated in 2019. Further information can be found on the Environment Agency website
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data

6. Equipment and Digital Content

Mobile Devices (Mobile Phones, Tablets and other Mobile Devices)

- Mobile devices brought in to College are the responsibility of the device owner. The College accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.

- No images or videos or recordings should be taken on mobile devices without the prior consent of the person or people concerned
- All visitors are requested to keep their phones on silent
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided. All mobile device use is to be open to monitoring scrutiny and the DSP is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary
- The College reserves the right to search the content of any mobile devices on the College premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobiles devices may be searched at any time as part of routine monitoring

Storage, Synchronisation and Access

Personal device accessed with a College owned account:

- The device has a College provisioned account and all app and file use is in line with this policy.

College device accessed with a personal account:

- If personal accounts are used for access to a College owned mobile device, staff must be aware that College use will be synchronised to their personal cloud, and personal use may become visible in College systems and in the classroom
- PIN / ID access to the device must always be made known to the Network Manager
- Exit process – when the device is returned, the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse

Students' Use of Personal Devices

- Phones and devices must not be taken into examinations. Students found in possession of a mobile device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences

Staff Use of Personal Devices

- Staff should not use their own personal mobile phones or devices in a professional capacity, such as for contacting students, young people or their families within or outside of the College setting
- Staff will be issued with a College mobile phone where contact with students, parents or carers is required, for instance for off-site activities
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose

Digital Images and Video

In this College:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the learner agreement form at enrolment
- We do not identify students in online photographic materials or include the full names of students in the credits of any published College produced video materials/DVDs; unless permission has been granted
- Staff are aware of the College's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of students
- If specific pupil photos (not group photos) are used on the College web site, in the prospectus or in other high profile publications, the College will obtain individual parental or learner permission for its long term, high profile use
- The College restricts access to social networking sites during normal lesson times
- Students are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger students
- Students are advised to be very careful about placing any personal photos on any social online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information
- Students are taught that they should not post images or videos of others without their permission. Students are advised about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. Students are advised on the need to keep their data secure and what to do if they are subject to bullying or abuse

Staying Safe Online

Advice for Students:

The internet is all encompassing. It can lay the world at our feet; but just as in the real world, not every internet user has our best interests at heart. There are people out there who want to steal from you or inflict damage to your computer, tablet or phone:

- They want to steal your identity so they can commit crimes and implicate you
- They want to sell you things that don't exist or make you do things you don't want to
- They also want to take over your computer or phone and use it when you're not looking. Stay safe and follow the tips below to help you stay safe
- you answer emails, texts or phone calls, make sure you keep your location and identity private, unless you really know the person well
- Never disclose personal information. If they just know your birthday or your pet's name, they might use these things to impersonate you
- Keep your passwords safe. Anyone who has your password can go into your site or your online presence and corrupt your data
- If you are using a computer in an Internet Café, or one that belongs to someone you don't know – be careful. They can have things like 'spyware' on them. This takes your details secretly and passes it on to people who may cause you harm or upset

- Spyware records what letters and numbers you have pressed on the keyboard (like passwords) and sends it to whoever set the key logger up. Think carefully about the information you are sending on these public computers and try to avoid giving any really personal information when using devices that aren't your own
- They may have viruses too, so if you send a friend an email you could infect them as well
- Your personal equipment - a phone or a computer, contains lots of your private information; messages, photographs, homework, phone numbers, texts and other things you like. If you leave them unlocked, anyone can see these things. They could delete, steal or publish them online without your knowledge. Always lock your devices when you're not using them
- Passwords are good way of staying safe but, you can't rely on just one. Have a different password for each system you use. If you only have one password and someone finds out what it is, they will be able to access all of your sites, computers and phones
- Do not use applications that suggest "remember password for this site". The risk will be that the next person that uses your computer will have access to your account. Passwords are there to protect you, if you let the site, the browser or your computer remember it there's no point having it
- Don't give away details about yourself and don't share things like your birthday or where you live
- Be wary of using any Open or Public Wi-Fi signal. They may not be secure and this may allow hackers to gain access to your device your device
- Ensure that you only download apps from the official store for your device. Apps are useful but unless they come from a known source, they may not be safe. Apps can harm your phone or device in a similar way to viruses.

Documents Associated with this Policy

Child Protection and Safeguarding Policy and Procedure
Acceptable Use Agreement (Staff)
Acceptable Use Policy (Students)

Document History			
Author:	Director IT & MIS	**Ref and Document Version:**	Online Safety and Use of Technology Policy and Procedure – V2
Approval:	College Executive	**Approval Date:**	December r2020
Review Date:	December 2023		
Publication:	Staff Intranet Student Intranet		

Quality Assurance	
This Policy and Procedure maps to the following external quality assurance frameworks	
Framework	**Framework Section Reference(s)**
Education Inspection Framework	
MATRIX	
QAA	
QIA	
ESFA	

Key Changes to Document

All Myerscough College Policies are subject to screening for Equality Impact Assessment

Equality Impact Assessments are carried out to see whether the policy has, or is likely to have, a negative impact on grounds of: age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, marriage or civil partnership, sex or sexual orientation

Myerscough College not only fulfils its legal position in relation to current and future equality legislation, but additionally goes beyond compliance in providing and promoting "Opportunities for all to succeed", free from any aspect of discrimination, harassment or victimisation.

All staff have a duty of care to look after the interests of and support their colleagues. *This policy takes account of* our commitment to eliminating discrimination, identifying and removing barriers and providing equal opportunities for our learners, staff and visitors to ensure that no one feels excluded or disadvantaged.

Safeguarding, Learner Protection and Prevent

All staff have a responsibility to support and promote the College's commitment to providing a safe environment for students, staff and visitors. Additionally, all staff have a responsibility to report any safeguarding or Prevent issues to the Designated Senior Lead for Safeguarding and Prevent.