Moat Community College

E-Safety Policy

Vision Statement

Moat Community College embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, Moat Community College aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the college and to personal devices owned by staff and students while on the college premises.

Related Documents:

Acceptable Use Policy for Staff

Acceptable Use Policy for Students

Publicising e-Safety

Effective communication across the college community is key to achieving the college vision for safe and responsible citizens. To achieve this we will:

- Make this policy, and related documents, available on the college's SharePoint at: http://www.moat.leicester.sch.uk
- Introduce this policy, and related documents, to all stakeholders at appropriate times. This will be at least once a year or whenever it is updated

Roles and Responsibilities

The Principal and Governors have ultimate responsibility for establishing safe practice and managing e-Safety issues at our college. The designated senior person for child protection is David Buckle.

All members of the college community have certain core responsibilities within and outside the college environment. They should:

- Use technology responsibly.
- Accept responsibility for their use of technology.
- Model best practice when using technology.
- Report any incidents to senior leadership.
- Understand that network activity and online communications are monitored, including any personal and private communications made via the college network.
- Be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action.

Physical Environment / Security

The college endeavours to provide a safe environment for the whole community. We review both physical and network security regularly as well as monitor who has access to the system.

- Anti-virus software is installed on all computers and is updated regularly.
- A two tier Filtering system – utilizing Impero monitoring and control software and Lightspeed web filtering, is in place and is managed by the ICT technical support team.
- The college uses Impero on all Windows and OS X computers to ensure compliance with the Acceptable Use Policies.
- All staff are issued with their own username and password for network access. Visitors / Supply staff are issued with temporary ID's and the details recorded in technicians office, in accordance with both the *'Network Security Policy'* and *'Acceptable Use Policy'*.

- All students are issued with their own username and password for network access and understand that this must not be shared. Guidelines and rules are laid out in both the *‘Network Security Policy’* and *‘Acceptable Use Policy’*. All students must agree and sign before accessing ICT resources.

Mobile / emerging technologies

- Teaching staff at the college are provided with a laptop for educational use and their own professional development. All staff understands that the *Acceptable Use Policies* apply to this equipment at all times.
- To ensure the security of the college systems, all visitors and staff bringing in personal mobile devices to access the colleges network resources should seek permission from the colleges network manager.
- Staff understand that they should use their own mobile phones sensibly and in line with colleges e-safety policy digital media section.
- The Education and Inspections Act 2006 grants the Principal the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Principal will exercise this right at their discretion
- Pictures / videos of staff and students should not be taken on personal devices.
- New technologies are evaluated and risk/benefit assessed before they are introduced to the college community

Mobile Phone Misuse

- All UK mobile operators have nuisance call centres set up and/or procedures in place to deal with such instances. The responses may vary but possibilities for the operator include changing the mobile number of the person being bullied so that the bully will not be able to continue to contact them without finding out their new number. It is not always possible for operators to bar particular numbers from contacting the phone of the person being bullied, although some phone handsets themselves do have this capability. Action can be taken against the bully’s phone account (e.g. blocking their account), only with police involvement. For further information please contact your mobile phone provider.

E-mail

Moat uses Microsoft Office 365 Outlook Web Access as its e-mail system. This provides two levels of security.

- Anti-virus/anti-malware protection is built in to Office 365.
- Staff can use the encrypted email features to send messages secure from interception.

Published content

The Principal takes responsibility for content published on the college web site but delegate's general editorial responsibility to the ICT manager. Subject teachers and area co-ordinators are responsible for the editorial control of work published by their students.

- The college will hold the copyright for any material published on the college web site or will obtain permission from the copyright holder prior to publishing with appropriate attribution.

Digital Media

We respect the privacy of the college community. If we have direct instructions not to publish or share a specific student's image or video, then we will refrain from doing so in the public space. By default we will ask for the permission of staff, parents, carers and students to share any images or video for promotional aspects of college life in accordance with the *'Acceptable Use Policy'* and other related documents listed within this policy. Parental consent will be sought and recorded on SIMS.

- Photographs and/or videos of students in college must only be taken using the college's equipment. Personal cameras and or phones should not be used.

Social Networking and online communication

The use of social networking sites and online communication is currently restricted, with the exception of the college's SharePoint system, which is monitored internally.

Guidance is provided to the college community on how to use these sites safely and appropriately. This includes

- Not publishing personal information.
- Not publishing information relating to the college community.
- Ensure appropriate privacy settings are applied.
- How to report issues or inappropriate content on the sites listed below.

Guidelines / Good Practice

It is normally possible to block/ignore particular users on social networking sites, which should mean the user can stop receiving unwanted comments. Users can do this from within the site.

Many social network providers also enable users to pre-moderate any comments left on their profile before they are visible by others. This can help a user prevent unwanted or hurtful comments appearing on their profile for all to see. The user can also set their profile to 'Private,' so that only those authorised by the user are able to access and see their profile.

If social networking sites do receive reports about cyber bulling, they should be able to investigate and may remove content that is illegal or breaks their terms and conditions in other ways. By reading the terms and conditions you will be able to see information on what is inappropriate and unacceptable behaviour, as well as providing prominent safety information so that you know how to use the service safely and responsibly.

It is advised to report any incidents of unpleasant comments posted on these sites and also take steps to have them removed. The procedure for different sites is provided below.

Facebook

You have to be at least 13 years old to sign up to Facebook and students below this age should not attempt to bypass the age verification controls used. There are different ways to stop bullying on Facebook, depending on the type of bullying. You can remove tags or block people who are sending you nasty messages. You can also report abusive posts or groups so Facebook can take them down. Reports are anonymous so the person doing the bullying won't know who reported it.

The way to report abuse changes depending on what you are reporting. https://www.facebook.com/help/420576171311103/

It's a really good idea to set your profile to 'friends only' so that you can't be on the end of bullying from people you don't know.

You can find the Terms of Service by following this link: http://www.facebook.com/terms.php?ref=pf

YouTube

YouTube is currently blocked in college for students. We are looking at allowing access to YouTube for Schools but realise that this does not include many of the educational resources that staff and students want to view. YouTube can be a great online video community – but it's important to follow their safety guidelines. Bullying on YouTube could happen through videos themselves or through the comments that people post on videos.

YouTube has a very strict policy on what's allowed in videos, comments and general behaviour. If the bullying is in a video you can report it by clicking the 'flag' button underneath the video. If you want to report cyber bullying or abuse through comments or private messages then you can use YouTube's reporting tool link: http://www.youtube.com/yt/policyandsafety/reporting.html

Instagram

Instagram is a service for sharing photos with your friends, but some people try to use it for cyber bullying instead. Sometimes people might write nasty comments on an image or upload embarrassing photos of someone. Instagram is automatically set to public so that anyone can see your images - even if you don't know them. It's much easier to stop bullying if your profile is private. When your profile is private, anyone who wants to follow you and see your photos has to send you a request - which you can ‘approve’ or ‘deny’. This way you can control who sees your photos and can make sure only your friends can talk to you on Instagram. You should also report anyone who is being abusive to you by using the link below: http://help.instagram.com/165828726894770/

Snapchat

Snapchat is different from other photo sharing apps because when you send an image, it will only last between 1 and 10 seconds before being deleted. Remember that a number of different tools are available that allow users to permanently save Snapchat photos so they are not deleted.

If someone is bullying you on Snapchat, blocking them will stop them from sending abusive messages. You can also report bullying to Snapchat - they may be able to help stop it. https://support.snapchat.com/co/harassment

Tumblr

Tumblr is a great blogging and social network site which lets you post and share your interests with others.

People on Tumblr can ask you questions anonymously, which means you don’t know the identity of the person asking the question. Sometimes people decide to send abusive or hurtful messages to other people on Tumblr. If someone sends you an abusive question or comment on Tumblr, you can block the user on the Tumblr ‘ignore’ page. https://www.tumblr.com/ignore

Twitter Appropriate Usage Policy

1. All tweet requests will be submitted by email or through SharePoint to: twitter@moat.leicester.sch.uk and may be accompanied by one photo or web address (link).
2. Staff assume responsibility for communicating with a public audience and representing the college when submitting tweet requests to whole college admins.
3. Ultimate responsibility for the content of any tweet lies with the admin publishing the tweet.

4. Admins may deny a tweet request, and will provide prompt written or verbal reasoning to the member of staff requesting the tweet.
5. Content of tweets must always relate to Moat or events that Moat is participating in.
6. Photos and/or links submitted to accompany tweets must be in accordance with the esafety policy.
7. Tweets naming students may only be published with the express written or verbal permission of the student concerned, or that of a parent/guardian.
8. Administrators will block any users bringing the college into perceived disrepute by comments made regarding @MoatCollege tweets.

   Justification for such action will only be provided outside of exceptional circumstances.
9. College teams wishing to tweet for themselves must:
   a. Register an appropriately-named account on Twitter.com
   b. Provide college administrators with this account name and its password.
   c. Nominate a team member to be responsible for publishing tweets.
   d. Adhere to all aspects of the Moat Twitter AUP in lieu of the whole-college administrators, with the following exception:
      i. College teams may address individual teaching or extracurricular groups, but may not use twitter to communicate with individual students or staff.
      ii. Staff will not use Twitter's private messaging facility to communicate with current college students under any circumstances.

Data Security / Data Protection

Personal data will be recorded, processed, transferred and made available in line with the *'Data Protection Policy'.*

Data stored on the college systems is password protected and encrypted in line with the *'Network Infrastructure Security Policy'.*

All staff laptops will have encryption functionality enabled.
"Encrypt any personal or sensitive data that is removed or accessed from outside an approved secure space."

Encryption is the process of scrambling data to make it unreadable to anyone except those authorized to do so.

FileVault 2 is the encryption method used. This encrypts the entire hard drive and allows remote or automated data wipe should a device be lost or stolen.

Responding to incidents

Internet usage/Filtering

- A two tier Filtering system – using Impero and Lightspeed is in place and is managed by the ICT technical. All staff and students understand that if an inappropriate site is discovered it must be reported to the ICT technical team who will fill out an e-safety incident report and block it internally while alerting the colleges child protection representative to relevant issues.

- The college uses Impero on all network computers to ensure compliance with the Acceptable Use Policy. If students access inappropriate content a screenshot is generated and a report is sent via email to the ICT Network Manager. If screenshots are generated by staff then a member of the senior management and or the Principal will be notified.

- Requests for changes to the filtering will be directed to the ICT technical team in the first instance who will then forward these on to the ICT Network Manager. Change requests will be recorded in the e-Safety log for audit purposes.

- Breaches of this policy by staff will be investigated by the Principal teacher. Action will be taken under Leicester City Council's Disciplinary Policy where a breach of professional conduct is identified. Incidents will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct. All monitoring of staff use will be carried out by at least 2 senior members of staff.

- Student policy breaches relating to bullying, drugs misuse and abuse must be reported to the nominated child protection representative (David Buckle) and action taken inline with college anti-bullying and child protection policies.

- Minor student offenses, such as being off-task visiting games or email websites will be handled by the teacher in situ by invoking the college behaviour policy.

- The Educations and Inspections Act 2006 grants the Principal the legal power to take action against incidents affecting the college that occur outside the normal college day and this right will be exercised where it is considered appropriate.