East Midlands Specialist College Group
E-Safety Project

Information and Learning Technology Acceptable Use Policy

Our policy

Under the Data Protection Act, the College, has a duty to protect personal data held on computer from unlawful use.

Information held in the College's ILT system are backed up daily and tapes are stored in a secure location away from the building in which the main servers are housed. This means that in the event of system failure, hardware failure, water damage, fire, theft, or vandalism, the data is not lost.

Anti-virus programmes are used to monitor files in use and a full anti-virus check is carried out continuously.

System and software updates are installed on computers and servers as and when required. This process is carried out to minimise disruption to users.

Our practices

College staff and learners may use the computer systems and related equipment for purposes relating to their education and work.

The College expects all its computer facilities to be used in a professional manner. These facilities are provided by the College at its own expense for its own business purposes. It is the responsibility of each user to ensure that this technology is used for proper business purposes and in a manner that does not compromise the College, its employees or its learners in any way.

In general, all users have a duty not to disclose information from or about the system, nor to carry out any unauthorised access or in any other way use, manipulate or alter the data held.

Accounts for use on the College network will only be created by members of the IT Support team and will only be issued at the request of relevant College managers. Users have restricted access depending upon their needs. Access to facilities on the network will depend upon the individual's role within the College or their learning programme.

Deletion of user accounts will only be performed by members of the IT Support team and will only be performed at the request of relevant College managers. All staff user accounts are deleted upon termination of their employment at the College. All users' work will be deleted from their respective accounts upon termination/completion of their employment or programme. Learners currently have access to generic accounts for use during their studies.

Account lock out – users accounts are locked after 3 failed attempts logging on to the network. Only the IT Support Team can unlock locked accounts. This procedure prevents potential hackers from having the freedom to try again and again to log onto the network.

It is the responsibility of the user to log off from the computer they are using when the following criteria apply.

- Break and Lunch times
- At the end of a working day
- When the user will be away from the equipment for any length of time

Users should not transmit anything in an e-mail, fax or text message that they would not be comfortable writing in a letter or a memorandum. It should be noted that electronic messages are admissible as evidence in legal proceedings and have been used successfully in libel cases.

Users should never assume that internal messages are necessarily private and confidential, even if marked as such. Matters of a sensitive nature should not be transmitted by e-mail unless absolutely unavoidable.

E-mail messages, both sent and received, should be treated as non-confidential. Anything sent through the Internet passes through a number of different computer systems all with different levels of security. The confidentiality of messages may be compromised at any point along the way unless messages are encrypted.

Requests for support relating to College IT equipment must be passed to the ILT mentor or Administrator who will forward them to IT Support or access the telephone support service.

College users may not: -

- Send offensive, demeaning or disruptive messages. This includes, but is not limited to, messages inconsistent with the College's equal and diversity or inappropriate behaviour policies. Users should therefore not place on the system any message which would be regarded as personal and sensitive, potentially offensive or frivolous to themselves or to any recipient. If an individual receives mail containing material which is offensive or inappropriate it must be deleted immediately. Under no circumstances should such mail be forwarded either internally or externally. If in any doubt the individual should refer the matter to their own appraisal manager/Tutor without delay.
- Attempt to or access any part of the computer system for which they do not have the proper authorisation or where it is not part of their normal routine work/studies.
- Attempt to or bypass security/anti-virus measures set up to safeguard information and protect files.
- Read, modify, copy or delete any programs or other user's data without the proper authorisation.
- Install, change or remove any software without the prior approval.
- Copy, sell or distribute software in violation of international copyright laws.
- Use the computer resources for commercial purposes and/or for personal profit.
- Use the College's IT system for gambling activities (the Gambling Act 2005 defines betting and gaming).
- Use any part of the system to access, view, and distribute pornographic or obscene text or images.
- Use another individual's computer account and password (including e-mail account). All users must ensure that workstations are either locked or switched off before vacating their working area. If it is anticipated that another user may need access to some confidential files in their absence arrangements should be made for the files to be copied to another location which remains confidential but where the third party can access them.
- Disclose details of any computer account, e-mail addresses, passwords and system information to third parties without the proper authorisation
- Move or disconnect any computer equipment without the prior approval of the IT support technician or make changes to the installation or configuration.
- Bring in or use their own equipment or software without prior approval.
- Connect personal equipment to the College network such as Laptops, printers, USB devices without prior approval.

Any infringement of these regulations could result in disciplinary action and could, in certain circumstances, lead to civil or criminal proceedings.

The College reserves the right to use monitoring and restriction software on its systems and users should be aware that their use of the system might be monitored.

Internet Policy

Access to the Internet should be limited to matters relating directly to the individual’s employment/education. Unauthorised use of the Internet includes but is not limited to connecting, posting or downloading any information unrelated to employment/education and in particular pornographic material, engaging in computer hacking and other related activities or attempting to disable or compromise the security of information contained on the College’s computer systems.

Postings placed on the Internet may display the College’s address. For this reason individuals should make certain prior to posting information that the information reflects the standards and policies of the College. Under no circumstances should information of a confidential or sensitive nature be placed on the Internet.

Information posted or viewed on the Internet may constitute published material. Therefore, reproduction of information posted or otherwise available over the Internet may be done only by express permission from the copyright holder.

You must not commit the College to any form of contract through the Internet. Subscriptions to news groups and mailing lists are only permitted when the subscription is for a work-related or educational purpose. Any other subscriptions are prohibited.

When using the Internet from the College’s computer system users need to be aware of the following guidelines outlining acceptable and unacceptable usage.

Acceptable uses

Users may use the Internet for purposes *relating to their work/studies* this will include but not be limited to the following activities: -

- Browse the World Wide Web
- Send/receive E-mail
- Transfer work/education related files and documents to and from the College’s systems

Please remember in any communication that you are representing the College.

Unacceptable uses

Whilst using Landmarks’ equipment users may not: -

- Deliberately view, download or distribute pornographic or obscene text or images
- Knowingly violate local, UK or European laws, particularly those relating to obscenity and copyright
- Use another company or individual’s property without their prior approval
- Download, use or distribute unlicensed software
- Use the Internet for personal or financial gain
- Access gambling sites or auction sites.

Please be aware that deliberate misuse of the Internet/email will result in disciplinary action, possibly leading to dismissal/exclusion.

Monitoring/Restrictions

Email & Internet

The College has email/internet monitoring/filtering software in place and reserves the right to intercept any e-mails or monitor access to web sites on the internet for the following reasons; record keeping purposes, checking compliance with regulations, quality control or staff training, preventing or detecting crime, investigating or detecting unauthorised use, checking for viruses or other threats to the system.

Advice and Guidance when using social networking sites

The college understands the popularity and usefulness of social networking sites and actively supports their use by learners on condition that:

- No offensive or inappropriate pictures are posted on to any website whilst using Landmarks's internet access.
- No offensive or inappropriate comments are posted.
- Make sure any information you place on any website(s) does not violate Landmarks's Acceptable Use of Computers Policy. Learners must remember that they are representatives of Landmarks and are in the public eye. Please keep the following in mind as you participate on social networking websites.
- Before participating in any online community, understand that anything posted online is available to **ANYONE IN THE WORLD.** Any text or photos placed online become the property of the site(s) and is completely out of your control the moment it is placed online **- even if you limit access to your site.**
- You should not post any information, photos or other items online that could embarrass you, your family, or the College or possibly lead to prosecution. **This includes information that may be posted by others on your page – remember you are responsible for your website's contents.**
- Never post your home address, local address, phone number(s), birth date or other personal information. You could be a target of predators.
- Landmarks can and will monitor usage and websites accessed whilst using the College's internet access.
- Learners must be aware that they could face disciplinary action for violating the College's policy. Learners need to be aware the police and other law enforcement agencies also monitor Social Networking websites regularly.

Produced for the East Midlands Specialist College Group E-Safety Project
by Landmarks College
See our website for more! www.em-esafetyproject.co.uk