E-Safety Policy and Code of Practice

Policy:

- The requirement to ensure that staff and students are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work within this college are bound.
- This policy and its associated codes of practice apply to all college staff, volunteers and students. It is designed to clarify the acceptable usage; responsibilities and accountabilities, which need to be considered when accessing and using the e-mail; intranet and Internet systems.
- The College's email, Internet and intranet systems are primarily for business use. Reasonable personal use is permitted provided that this does not interfere with the performance of staff, volunteer or student duties. If the member of staff, volunteer or student is unclear about what constitutes reasonable use, they should consult their line manager or tutor. They may also seek guidance from the IT Systems Co-ordinator.
- E-mails sent and received by staff, volunteers or students may, as part of routine security checks, be inspected by the college IT Team.
- With the senior manager's permission, access to the College's email system from a home computer may be authorized. Staff, volunteers and students are responsible and accountable for their conduct during this time.
- This policy applies to all members of the college community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of college IT systems, both in and out of college.
- The College will ensure that staff and students will have access to the network to enhance their work and learning and will, in return, expect staff and students to agree to be responsible users through the relevant college Acceptable Use Policies

The College ensures:

- That staff and students will be responsible users (as set out in the Acceptable Use Policy) and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That college IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff and students are protected from potential risk in their use of ICT in their everyday work.

Through this policy and codes of practice, the college aims to protect staff, volunteers and students to ensure legal problems do not arise either for themselves or for the college, with particular reference to the following legislation:

- Human Rights Act 1998.
- Regulation of Investigator Powers Act 2000
- Telecommunications (Lawful Business Practice, Interception of Communications) Regulations 2000.
- Data Protection Act 1998
- Copyright, Designs & Patents Act 1988.
- Obscene Publications Act 1959.
- Protection of Children Act 1988.
- Criminal Justice Act 1988
- Computer Misuse Act 1999

This policy must be read in conjunction with the staff and student codes of practice and Acceptable Use policies. If further explanation or clarification is required, the individual must seek this from their line manager or tutor.

The failure to comply with the Policy may lead to disciplinary action.

Code of Practice

Roles and Responsibilities

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors Education and Student Welfare Sub Committee* receiving regular information about e-safety incidents and monitoring reports.

The **Principal** is responsible for ensuring the safety (including e-safety) of members of the college community, though the day to day responsibility for e-safety will be delegated to the Head of College Development and Safeguarding Officer.

The **Principal** and another member of the **Senior Management Team** should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a student or member of staff. (see intervention flowchart).

The **Head of College Development**

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the college e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with college IT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- attends relevant meetings of Governors sub committee
- reports regularly to Senior Leadership Team

The **IT systems coordinator** is responsible for ensuring;

- that the colleges IT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the college's networks through a properly enforced password protection.

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current college e-safety policy and practices
- they have read, understood and signed the college Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Head of College Development
- digital communications with students (email / Virtual Learning Environment (VLE) / voice) should be on a professional level

Safeguarding Officers are trained in e-safety issues and be aware of the potential for serious child/adult protection issues to arise from:

- sharing of personal data.
- access to illegal / inappropriate materials.
- inappropriate on-line contact with adults / strangers.
- potential or actual incidents of grooming.
- cyber-bullying.

Students are responsible for using the college IT systems in accordance with the Student Acceptable Use Policy

Training

- A planned programme of formal e-safety training is delivered as part mandatory safeguarding and boundaries and will be made available to staff.
- An audit of e-safety training within the college training quality audit needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the college e-safety policy and Acceptable Use Policies

Infrastructure, equipment and monitoring

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

- There will be regular reviews and audits of the safety and security of college IT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to college IT systems
- All users will be provided with a username and password by the IT systems Coordinator who will keep an up to date record of users and their usernames.
- The administrator passwords for the college IT system, used by the IT systems coordinator must also be available to the Director and Head of College Development and kept in a secure place
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details, and must immediately report any suspicion or evidence that there has been a breach of security.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the college systems and data.
- The college has provided enhanced user-level filtering through the use of the JANET and Sonic Wall filtering programs. In the event of the IT systems coordinator (or other systems staff) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head of College Development.
- Requests from staff for sites to be removed from the filtered list will be considered by the IT systems coordinator, behavioural support coordinator and Head of College Development.
- College IT technical staff regularly monitor and record the activity of users on the College IT systems and users are made aware of this in the Acceptable Use Policy. Remote management tools are used by staff to control workstations and view users' activity.
- The college infrastructure and individual workstations are protected by up to date virus software.
- The college prohibits the downloading of executable files and the installation of programmes onto college workstations.

Monitoring

This e-safety policy was approved by the *Governing Body / Governors Sub Committee* on:	
The implementation of this e-safety policy will be monitored by:	Director of College Development and College Senior Management Team
Monitoring will take place at regular intervals:	Once a term
The *Governing Body / Governors Sub Committee* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	3 times per year at education and student welfare board sub - committee meetings
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	24th March 2010
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Safeguarding Officer

The college will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of IT across the curriculum;

- in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT systems coordinator or behavioural support coordinator can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, but must follow college policies concerning the sharing, distribution and publication of those images. Those images should only be taken on college equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the college into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the college website
- Student's work can only be published with the permission of the student or parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes

- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- transfer data using encryption and secure password protected devices.

Communication

When using communication technologies the college considers the following as good practice:

- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person (students to their Tutor, Key worker or Personal learning mentor, Staff to their line manager) – in, accordance with the college policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content.

Unsuitable and inappropriate activity

Users shall NOT visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images.
- promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation.
- adult material that potentially breaches the Obscene Publications Act in the UK.
- criminally racist material in UK.
- pornography.
- promotion of any kind of discrimination.
- promotion of racial or religious hatred.
- threatening behavior, including promotion of physical violence or mental harm.
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the college or brings the college into disrepute.
- using college systems to run a private business.

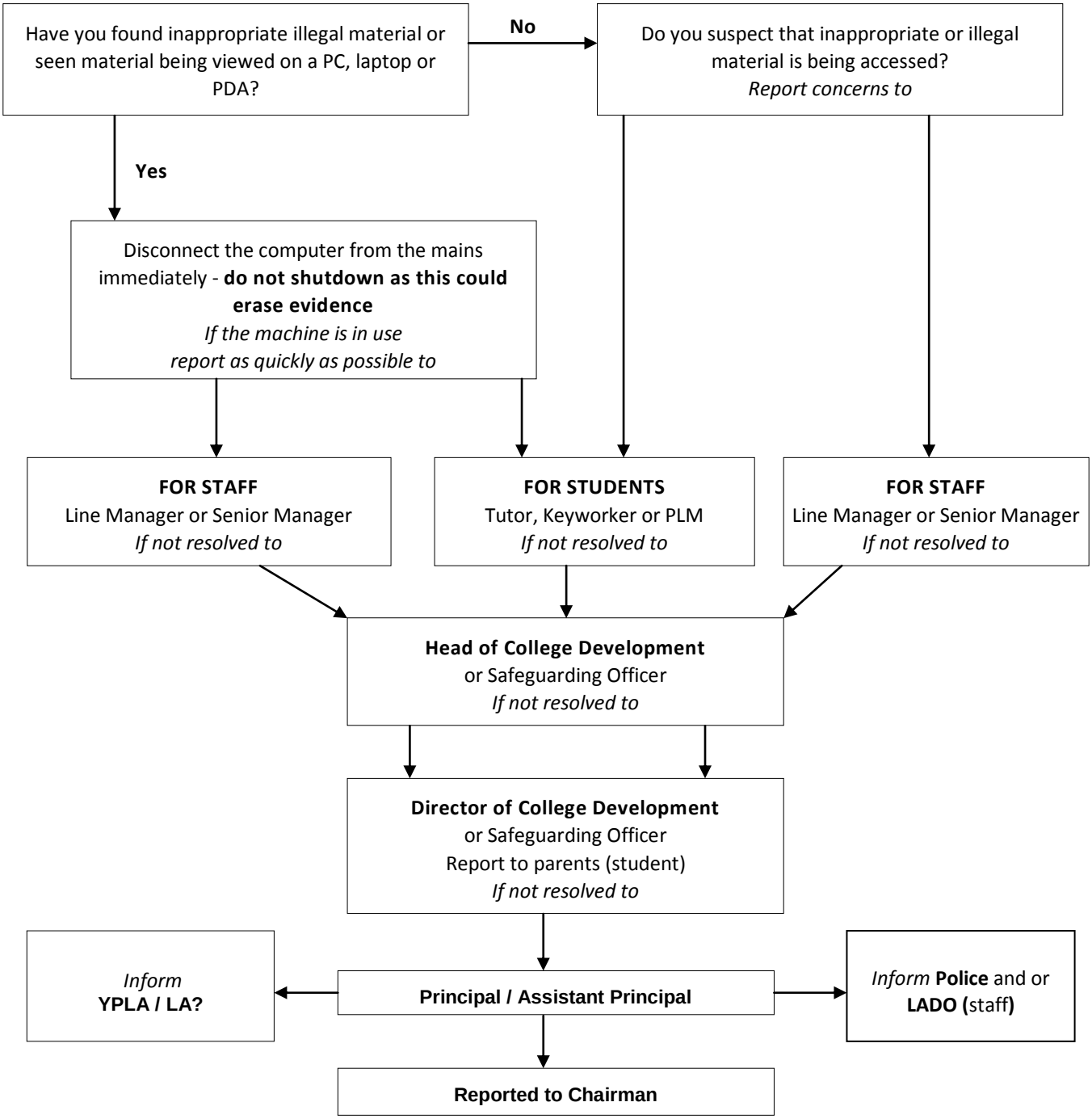
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the college.
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.
- revealing or publicizing confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords).
- creating or propagating computer viruses or other harmful files.
- carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet.
- file sharing.
- on-line gambling.

Users MAY visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- on-line gaming (educational)
- on-line gaming (non educational)
- on-line shopping / commerce
- use of social networking sites
- use of video broadcasting e.g. YouTube

Within context and with permission of tutor, key worker or personalized learning mentor

Responding to incidents of misuse



Students **Sanctions/Actions (Guidance to consider)**

Student Incidents:	Refer to teacher / tutor	Refer to Head of Department	Refer to Principal/Senior Manager	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. suspension or exclusion
➢ Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			✓	✓	✓	✓	✓	✓	✓
➢ Unauthorised use of non-educational sites during lessons	✓							✓	
➢ Unauthorised use of mobile phone / digital camera / other handheld device	✓							✓	
➢ Unauthorised use of social networking / instant messaging / personal email	✓							✓	
➢ Unauthorised downloading or uploading of files	✓				✓			✓	
➢ Allowing others to access college network by sharing username and passwords		✓			✓			✓	
➢ Attempting to access or accessing the college network, using another student's / pupil's account		✓			✓			✓	
➢ Attempting to access or accessing the college network, using the account of a member of staff			✓		✓			✓	✓

Student Incidents:	Refer to teacher / tutor	Refer to Head of Department	Refer to Principal/Senior Manager	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. suspension or exclusion
➢ Corrupting or destroying the data of other users		✓	✓		✓			✓	✓
➢ Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓				✓	✓		✓	
➢ Continued infringements of the above, following previous warnings or sanctions			✓		✓				✓
➢ Actions which could bring the college into disrepute or breach the integrity of the ethos of the college			✓		✓	✓			✓
➢ Using proxy sites or other means to subvert the college's filtering system			✓		✓			✓	
➢ Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓						✓	
➢ Deliberately accessing or trying to access offensive or pornographic material		✓	✓	✓	✓			✓	✓
➢ Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓						✓	

Staff **Sanctions/Actions (Guidance to consider)**

Staff Incidents:	Refer to line manager or and Safeguarding Officer	Refer to Principal	Refer to HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	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).	✓	✓	✓	✓	✓		✓	✓
➢ Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓				✓	✓		
➢ Unauthorised downloading or uploading of files	✓				✓	✓		
➢ 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	✓	✓	✓		✓	✓		✓
➢ Careless use of personal data e.g. holding or transferring data in an insecure manner	✓					✓		
➢ Deliberate actions to breach data protection or network security rules	✓	✓	✓		✓	✓		✓
➢ Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓		✓		✓	✓
➢ Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓		✓			✓		

Staff Incidents:	Refer to line manager or and Safeguarding Officer	Refer to Principal	Refer to HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
➢ Inappropriately using personal email / social networking / instant messaging / text messaging to carry out digital communications with students	✓	✓	✓			✓		
➢ Actions which could compromise the staff member's professional standing	✓	✓	✓			✓		
➢ Actions which could bring the college into disrepute or breach the integrity of the ethos of the college		✓					✓	✓
➢ Using proxy sites or other means to subvert the college's filtering system	✓				✓	✓		
➢ Accidentally accessing offensive or pornographic material and failing to report the incident	✓					✓		
➢ Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓			✓	✓
➢ Breaching copyright or licensing regulations			✓		✓	✓		
➢ Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓	✓	✓		✓	✓

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