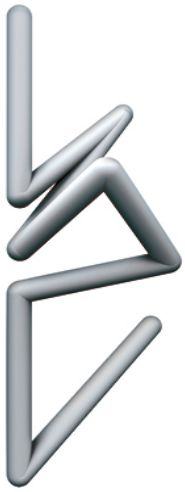
Lincoln University Technical College

A College for Science & Engineering



E-Safety Policy

www.lincolnutc.co.uk

Equality and Diversity Statement

Lincoln UTC strives to treat all its members and visitors fairly and aims to eliminate unjustifiable discrimination on the grounds of gender, race, nationality, ethnic or national origin, political beliefs or practices, disability, marital status, family circumstances, sexual orientation, spent criminal convictions, age or any other inappropriate grounds.

Policy Review

Policy Created: June 2014

Policy Reviewed: July 2016

Next Review: July 2019

LINCOLN UTC

E-SAFETY POLICY

CONTENTS

1. INTRODUCTION AND AIMS

- The college e-safety policy aims to create an environment where students, staff, parents, governors and the wider college community work together to inform each other of ways to use the Internet responsibly, safely and positively.
- Internet technology helps students learn creatively and effectively and encourages collaborative learning and the sharing of good practice amongst all college stakeholders. The e-safety policy encourages appropriate and safe conduct and behaviour when achieving this.
- Students, staff and all other users of college related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour.
- These agreements and their implementation will promote positive behaviour which can transfer directly into each pupil's adult life and prepare them for experiences and expectations in the workplace. The policy is not designed to be a blacklist of prohibited activities, but instead a list of areas to discuss, teach and inform, in order to develop positive behaviour and knowledge leading to a safer Internet usage and year on year improvement and measurable impact on e-safety. It is intended that the positive effects of the policy will be seen online and offline; in college and at home; and ultimately beyond college and into the workplace.

- This policy should also be read in parallel with:
    - The Safeguarding and Child Protection Policy
    - The Disciplinary Policy
    - The Acceptable Use Policy
      The Behaviour Policy

2. REVIEWING AND EVALUATING E-SAFETY AND ENSURING GOOD PRACTICE.

The e-safety policy will be monitored and evaluated annually by the standards sub-committee. We will monitor the application and outcomes of this policy to ensure it is working effectively.

Who does e-safety affect, who is responsible for e-safety and what are their roles?

UTC Management and e-safety

- College senior management is responsible for determining, evaluating and reviewing e-safety policies to encompass teaching and learning, use of college IT equipment and facilities by students, staff and visitors, and agreed criteria for acceptable use by students, college staff and governors of Internet capable equipment for college related purposes or in situations which will impact on the reputation of the college, and/or on college premises.
- e-safety policy is a result of a continuous cycle of evaluation and review based on new initiatives, and partnership discussion with stakeholders and outside organisations; technological and Internet developments, current government guidance and college related e-safety incidents. The policy development cycle develops good practice within the teaching curriculum and wider pastoral curriculum. Regular assessment of strengths and weaknesses help determine inset provision for staff and governors and guidance provided to parents, students and local partnerships.
- e-safety provision is always designed to encourage positive behaviours and practical real world strategies for all members of the college and wider college community.

UTC E-Safety Officer:

- The college has a Designated E-Safety officer, Ian Freeman who reports to the SLT and Governors and coordinates e-safety provision across the college. The committee liaises with SLT, the colleges Designated Safeguarding Lead and other senior managers as required.
- The college e-safety officer has a specific job description and person specification detailing the role, remit, qualifications and qualities required for the post.
- The college e-safety coordinator is responsible for e-safety issues on a day to day basis and also liaises with LA contacts, agencies, the DSL and college ICT support.
- The college e-safety coordinator maintains a log of submitted e-safety reports and incidents.
- The college e-safety coordinator audits and assesses inset requirements for staff, support staff and governor e-safety training, and ensures that all staff are aware of their responsibilities and the college's e-safety procedures. The coordinator is also the first port of call for staff requiring advice on e-safety matters.
- Although all staff are responsible for upholding the college e-safety policy and safer Internet practice, the e-safety Officer, and IT Technician are responsible for monitoring Internet usage by students and staff, and on college machines, such as laptops, used off-site and reporting concerns as necessary to the DSL.
- The e-safety Coordinator is responsible for promoting best practice in e-safety within the wider college community, including providing and being a source of information for parents and partner stakeholders.

Governors' responsibility for e-safety:

- At least one Governor is responsible for e-safety, and the college e-safety Officer will liaise directly with the Governor with regard to reports on e-safety effectiveness, incidents, monitoring, and evaluation. Any meetings or conversations will be minuted.

ICT support staff and external contractors:

- Internal ICT support staff and technicians are responsible for maintaining the college's networking, IT infrastructure and hardware. They need to be aware of current thinking and trends in IT security and ensure that the college system, particularly file-sharing and access to the Internet is secure. They need to further ensure that all reasonable steps have been taken to ensure that systems are not open to abuse or unauthorised external access, with particular regard to external logins and wireless networking.
- Support staff also need to maintain and enforce the college's password policy and monitor and maintain the Internet filtering.

- External contractors, such as VLE providers, website designers/hosts/maintenance contractors should be made fully aware of and agree to the college's e-safety Policy. Where contractors have access to sensitive college information and material covered by the Data Protection Act, for example on a VLE, college website or email provision, the contractor should also be CRB checked. It is best practice to keep long term maintenance and running of college VLEs, websites and email in-house, and only to outsource setup if required.

Teaching and teaching support staff:

- Teaching and teaching support staff need to ensure that they are aware of the current college e-safety policy, practices and associated procedures for reporting e-safety incidents.
- Teaching and teaching support staff will be provided with e-safety induction as part of the overall staff induction procedures.
- All staff need to ensure that they have read, understood and signed (thereby indicating an agreement) the Acceptable Use Policies relevant to Internet and computer use in college.
- All staff need to follow the college's social media policy, in regard to external off site use, personal use (mindful of not bringing the college into disrepute), possible contractual obligations, and conduct on Internet college messaging or communication platforms, for example email, VLE messages and forums and the college website.
- All teaching staff need to rigorously monitor pupil Internet and computer usage in line with the policy.
- Teaching staff should promote best practice regarding avoiding copyright infringement and plagiarism.
- Internet usage and suggested websites should be pre-vetted and documented in lesson planning.

Designated Safeguarding Lead:

- The Designated Safeguarding Lead needs to be able to differentiate which e-safety incidents are required to be reported to CEOP, local Police, LADO, social services and parents/guardians; and also determine whether the information from such an incident should be restricted to nominated members of the leadership team.

Students:

- Are required to use college Internet and computer systems in agreement with the terms specified in the college Acceptable Use Policies. Students are expected to sign the policy to indicate agreement, and/or have their parents/guardians sign on their behalf.
- Students need to be aware of how to report e-safety incidents in college, and how to use external reporting facilities.
- Students need to be aware that college Acceptable Use Policies cover all computer, Internet and gadget usage in college, including the use of personal items such as phones.
- Students need to be aware that their Internet use out of college on social networking sites such as Facebook is covered under the Acceptable Use Policy if it impacts on the college and/or its staff and students in terms of cyber bullying, reputation or
  illegal activities.

Parents and Guardians:

- It is expected that parents and guardians will support the college's stance on promoting good Internet behaviour and responsible use of IT equipment both at college and at home.

3. **E- SAFETY EDUCATION**

E-Safety education is part of the Life Guidance Curriculum for all students and includes how to deal with cyber bullying, how to report cyber bullying, the social effects of spending too much time online.
Parents will, where possible be provided with relevant e-safety information. Staff and Governors, will be provided with training as part of the induction process and ongoing CPD.

The E-Safety Officer should be the first port of call for staff requiring e-safety advice.

4. APPROPRIATE USE OF UTC SYSTEMS

Email

Students need to be made aware that messages are monitored and that the filtering system will detect, for example, inappropriate links, viruses, malware, and profanity. If staff email is monitored, the staff need to be made aware of this.

Personal information on the college website:

- No material defined as 'personal information' under the Data Protection Act should be used on a public college website.
- Colleges need to consider staff privacy issues carefully with regard to publishing staff email addresses, staff lists, photos of staff, staff qualifications and any other personally identifying information. If such information is included on a public website, it is best practise to instruct the web designer to include "noindex", "nofollow" and "noarchive" tags on the staff list webpages to ensure any information or images are not copied onto other websites, including search engines.
- It is better practice to include any information made up of lists of names and/or contact details (for example staff lists or lists students names for sports teams) on extranets or VLEs which are accessible to the college community, but not the wider public or search engines such as Google.

Inappropriate activity

The college needs to clearly define which online and network activities are appropriate and which are not. It is essential that the inappropriate activities are discussed and the reasoning behind prohibiting activities due to e-safety are explained to students in curriculum and co-curricular activities in order to promote responsible Internet use. As far as possible, restrictions need to reflect real life to precipitate a smooth transition to adult life in terms of the law, further education/university expectations, workplaces practices and public sector guidelines. The college 'Smoothwal'l is monitored, not blocked and any reports of students activity checked daily to highlight quickly any concerns.

5. E-safety incidents

If a student is found to access an inappropriate site or a site that raises a safeguarding concern, this is discussed with the student and parents as appropriate and letters sent home (Appendix). Where the access is by a staff member, this will be dealt with via the disciplinary and safeguarding policies.
If illegal material is found or accesses, reports can also be made to the IWF - www.iwf.org.uk/report. Police will be contacted and the Safeguarding and Child Protection Policy followed. If there is a child protection issue, the Safeguarding and Child Protection Policy will apply.

6. E-safety and the Law:

Computer Misuse Act 1990, sections 1-3
Data Protection Act 1998
Freedom of Information Act 2000
Communications Act 2003 section 1,2
Protection from Harassment Act 1997
Regulation of Investigatory Powers Act 2000
Copyright, Designs and Patents Act 1988
Racial and Religious Hatred Act 2006
Protection of Children Act 1978
Sexual Offences Act 2003
The Education and Inspections Act 2006 (Head teachers have the power "to such an extent as is reasonable" to regulate the conduct of students off site. Also, staff can confiscate mobile phones if they cause disturbance in class breach the college

7. **Useful links to external organisations:**

Ofsted:
- www.gov.uk/government/publications/college-inspection-handbook

DfE:
- www.gov.uk/government/groups/uk-council-for-child-Internet-safety-ukccis

CEOP:
- www.ceop.police.uk/safety-centre/
- childnet-int.org/

UK Safer Internet Centre:
- www.saferInternet.org.uk/safer-Internet-day
- www.saferInternet.org.uk/

Internet Watch Foundation:
- www.iwf.org.uk
- www.iwf.org.uk/members/get-involved

Links to training and resources:

E-safety Support: online refresher training www.e-safetysupport.com/online_training
CEOP: www.ceop.police.uk/training/
NAACE: e-safety online training: www.naace.co.uk/ictcpd4free
EPICT: offline and online e-safety training: www.epict.co.uk/#!esafetyinfo/cq8q

Movies and presentations:
www.swgfl.org.uk/Staying-Safe/e-safety-Movies
www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware

Other publications:
- Safer children in a digital world: the report of the Byron Review (PP/D16(7578)/03/08), DCSF and DCMS, 2008; http://webarchive.nationalarchives.gov.uk/20100202100434/dcsf.gov.uk/byronreview/.
- Ofcom's response to the Byron Review, Ofcom, 2008; http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/byron/.

Appendix:

Lincoln UTC
A college for Science and Engineering

Dear…….

As I am sure you are aware, at Lincoln UTC we have monitoring and filtering systems in place to ensure the appropriate use of our IT systems. However, our prime concern is to protect and maintain the safety of all our students.

These systems have highlighted that on DATE at TIME NAME has accessed, whilst on site, the website ……..

Accessing sites such as these is not acceptable nor compatible with the UTC 'Acceptable Use Policy' that all students have signed. Continued attempts to access this site or similar could result in ……. losing IT privileges, including internet access. I appreciate and understand that instances such as this can sometimes be accidental or due to innocent curiosity. However, we take our safeguarding responsibilities, including E-Safety, very seriously, and therefore believe that the proper action is to bring this to your attention.

If you would like to discuss this further or require additional information or support then please do not hesitate to contact me on 01522 775990, or email vweaver@lincolnutc.co.uk.

Kind regards

Vicky Weaver
SENCO and DSL

Lincoln UTC
A college for Science and Engineering

Dear…

As I am sure you are aware, at Lincoln UTC we have monitoring and filtering systems in place to ensure the appropriate use of our IT systems. However, our prime concern is to protect and maintain the safety of all our students.

These systems have highlighted that on DATE at TIME NAME has accessed, whilst on site, the website ……..(HYPERLINK)

I appreciate and understand that this may have been accidental or due to innocent curiosity. However, we take our safeguarding responsibilities to students very seriously and therefore believe that the proper action is to bring this to your attention.

If you would like to discuss this further or require support or additional information then please do not hesitate to contact me on 01522 775990, or email vweaver@lincolnutc.co.uk.

Kind regards

Vicky Weaver
SENDCO and DSL