Safe E-Learning and Acceptable ICT Use Policy

Policy Date:	September 2017		**Version:** 1.1		
Policy Review Date:	September 2018		Head Teacher: Anne Gregory	Signature: AG	Date: 25.04.18
Ratified by Governing Body:					
Chair of Governors: K Mistry			Signature: K Mistry		Date: 26.04.18

Safe E-Learning

Section 1 - Introduction

- The Internet and other digital and information technologies are valuable and powerful tools which open up new opportunities for everyone.

- Electronic communication enables teachers and students to learn from each other by stimulating discussion, promoting creativity and stimulating awareness of context to promote effective learning.

- All adults working in schools are required to ensure that children and young people are able to use the Internet and related communication technologies appropriately and safely as part of their wider duty of care to which all who work in colleges are bound.

- All adults and students are required to take the necessary steps to ensure their own safety when using digital and information technologies.

- Safe Internet practices must be embedded into the culture of our college. All college staff have a duty to ensure that students using ICT, in any context, are reminded about appropriate behaviour on a regular basis.

- ICT can offer many positive social and educational benefits to young people but unfortunately there are a number of dangers. For example;

    - Students are very vulnerable and can expose themselves to danger with or without knowing when using the internet or other technologies and can even find themselves involved in illegal activities.
    - Students may initiate some issues outside college that may have influence or be brought into college and so we must consider use of students' own equipment as well as e.g. bullying via chat or text messages.

- We must teach students and staff to use these technologies safely.

- To be safe, when using the internet and related technologies, both in and out of school, students and of course staff, must take personal responsibility. This involves;

    - developing appropriate behaviours
    - asking questions about sources of data
    - developing and using critical thinking skills
    - reporting abuses
    - not simply relying upon the automatic blocking of potential threats.

Section 2 - Risk Assessment – Some of the risks

1. **Copyright infringement** – copyright law applies on the internet but is often ignored and students download and swap music files, cut and paste homework assignments from other's work.

2. **Obsessive use of internet and ICT** – factors such as spending a significant amount of time online, deterioration of the quality of college work, diminished sleep time or negative impacts upon family relationships may all be indicators that the internet is taking too high a priority in the student's life.

3. **Exposure to inappropriate materials** – eg pornographic, hateful or violent in nature, encouraging activities that are dangerous or illegal or are just age-inappropriate or biased. Extreme political, racist or sexist views can be spread to give a distorted view of the world.

4. **Inappropriate or illegal behaviour** – This may include;

    a. **On line bullying** - groups or cliques can form online, and activities that begin as harmless fun can escalate into something much more serious. Online bullying is perceived as an anonymous method of tormenting victims, at any time day or night. A young person may receive email, chat or text messages which may not put them in physical danger but can embarrass, upset, frighten or depress them. This can lead to damage of self-esteem and may pose a threat to their psychological wellbeing.
    b. Identity theft
    c. Participation in hate or cult websites
    d. **Buying and selling stolen goods** are more serious activities that can occur.
    e. **Access to the following type of sites**;
        i. online gambling,
        ii. suicide sites
        iii. sites for the sale of weapons
        iv. hacking sites
        v. sites providing recipes for drug or bomb making.
        vi. pornographic sites - Viewing of indecent images via websites is something to be alarmed about. Any concern relating to criminally obscene or criminally racist content should be reported to the police.

5. **Physical danger and sexual abuse** – this is the most worrying and extreme risk associated with the use of the internet and other technologies. A criminal minority use the internet and related services eg chat rooms to make contact with young people to persuade them into sexual activity. The techniques used are on-line enticement, 'grooming' or child procurement. A young person can provide information on line that can personally identify them or others or they can arrange to meet people on-line thereby posing a threat to themselves or family or friends.

6. **Inappropriate or illegal behaviour by college staff** – Unfortunately it has occurred, very infrequently and in other colleges, where staff have been involved in inappropriate or illegal behaviour relating to ICT use. This could include;

    - viewing or circulating inappropriate material via e-mail, or more serious activities such as
    - viewing, possessing, making or distributing indecent/pornographic images.

    If found this will result in disciplinary action by the college or local authority. If illegal activities are found, the college has a duty to consult with police at the earliest opportunity and any evidence must be preserved. We therefore have a responsibility to educate staff as to acceptable behaviours on-line and to monitor networks for evidence of inappropriate activity.

Scetion 3 - Principles in Ensuring a Safe ICT Learning Environment

It is vital that The City of Leicester College provides a safe learning environment for all students at the college. This must include:

- An infrastructure of whole-college awareness, designated responsibilities, policies and procedures
- An effective range of technological tools
- A comprehensive internet safety education programme for the whole college community

It is particularly important to ensure that;

a. Everyone is aware of the issues and how they impact upon our college environment and the students.
b. There is an education programme that is continuous and provides continuous information about emerging technologies that affect the student's teaching and learning.
c. Students and staff are able to recognise when they are in danger and protect themselves
d. All staff and students are aware of their responsibilities with regard to their own safety and in the case of adults for the students in their care.
e. College policies and procedures must be followed at all times.
f. College polices and procedures should be regularly reviewed by all stakeholders and should take account of any new and emerging technologies and changes in local circumstances.
g. There are appropriate systems that the college has in place to safeguard students and staff these include:
    i. A firewall and virus protection. (ISP and college)
    ii. Forensic software that can monitor and keep track of downloads, inappropriate websites.
    iii. Filtering to minimise access to inappropriate content via the college network (ISP and college)
    iv. Observant adults and students.

Section 4 - Roles and Responsibilities

Internet Safety Co-ordinator – this is the senior manager with responsibility for internet safety management (College Leader New Technologies).

- The Internet Safety Co-ordinator is responsible to the head teacher and via the head the governors.
- The Internet Safety Coordinator;
    a. Works with the Headteacher and Internet Safety Team to ensure appropriate policies and procedures are reviewed and developed within the college.
    b. Works with the Head of ICT and other leaders within the college responsible for the curriculum to establish and maintain a safe ICT learning environment.
    c. Works with others to review and advise on internet safety policies. Leads on the development of management protocols for any incidents where internet safety is breached.
    d. Leads the development of the following with appropriate groups/people;
        i. staff development programme which addresses the benefits and risks of communication technologies. Staff have professional responsibilities for student safety in ICT use.
        ii. a programme for students regarding Internet Safety and appropriate use of ICT for such areas as research through ICT dept and PSHE.
        iii. a parent/carer awareness programme and it has been suggested that these information programmes for parents/carers be included on review days if possible.
    e. Maintains a log of any incidents relating to internet safety in the college and analyses the log to make recommendations for review of policy and use of technologies on the basis of emerging trends.
    f. Updates the Governing Body on current internet safety issues and progress.
    g. Laises with outside agencies as appropriate.
    h. Informs the Head teacher of any serious breaches in policy or procedure. These will be dealt with by the Headteacher, Governors or LA as appropriate. Police will be contacted if it is suspected that a criminal offence has been committed. Evidence must be secured and preserved as soon as possible.

Head teacher

The Head teacher delegates to the Internet Safety Co-ordinator and ensures that they have the authority and time to carry out these duties effectively.

The Head teacher (AMG):

- Supports the Internet Safety Co-ordinator and the Internet Safety Management team in creating an internet safety culture within the college, including speaking to staff and students in support of the programme
- Ensures that the Governing Body is informed of issues and policies
- Ensures funding is available to support internet safety activities for both technical infrastructure and inset training
- Promotes internet safety across the curriculum

Governing Body

Governing Bodies have statutory responsibilities for child protection and health and safety.

The Governing Body should:

- Develop an awareness of issues, risks and benefits regarding the use of ICT in the college
- Develop an understanding of existing college policies, systems and procedures for maintaining a safe ICT learning environment and supporting the Headteacher and Internet Safety Co-ordinator in implementing these
- Support the Headteacher and Internet Safety Co-ordinator in developing an appropriate strategy and plan for dealing with the media should any serious incidents occur
- Ensure that funding is available for internet safety solutions and training
- Promotes internet safety to parents/carers and provide updates on internet safety policies

Lead Education Technologist (LET)

The LET (C. Ryan) should:

- Work closely with the Internet Safety Co-ordinator to ensure that educational and technological aspects of internet safety support and compliment each other
- Carry out regular checks for indicators of misuse.
- Report immediately any case of indecent material accessed, even if it is only suspected, to the Internet Safety Co-ordinator/Headteacher who will contact police. If this is the case, no technical action should be taken by the Network Manager or any other staff member. Failure to secure and preserve evidence, if proven, may constitute a criminal offence in itself.
- Manage the network to trace inappropriate use, should any seriously inappropriate or age-restricted material be accessed, to remove the material from the college's network eg blocking of website. Technical systems and procedures should be reviewed immediately following an event to prevent them happening again.
- Report to the Internet Safety Co-ordinator or Headteacher regarding offending materials that can be traced back to individuals so that the appropriate disciplinary procedure can be followed. (If a student is involved Behaviour Support will then be informed to follow up with disciplinary action)
- Ensure appropriate and effective electronic security systems are in place eg filtering, monitoring and firewall technology
- Maintain an appropriate level of professional conduct in their own, and their team's internet use both within and outside college.

ICT Technicians

ICT Technicians should:

- Work closely with the LET to ensure that educational and technological aspects of internet safety support and compliment each other
- Report immediately any case of indecent material accessed, even if it is only suspected, to the Internet Safety Co-ordinator/Headteacher who will contact police. If this is the case, no technical action should be taken by the Network Manager or any other staff member. Failure to secure and preserve evidence, if proven, may constitute a criminal offence in itself.
- Follow procedures to trace inappropriate use on a regular basis, should any seriously inappropriate or age-restricted material be accessed, to remove the material from the college's network eg blocking of website.

Technical systems and procedures should be reviewed immediately following an event to prevent them happening again.

- Report to the Internet Safety Co-ordinator or Headteacher regarding offending materials that can be traced back to individuals so that the appropriate disciplinary procedure can be followed. (If a student is involved Behaviour Support will then be informed to follow up with disciplinary action)
- Ensure appropriate and effective electronic security systems are in place eg filtering, monitoring and firewall technology
- Maintain an appropriate level of professional conduct in their own internet use both within and outside college.

Hub Leaders

Hub Leaders should:

- Outline the procedures that staff are expected to follow, especially in relation to reporting incidents where internet use policies have been breached.
- Ensure staff in the faculty/department are aware of the requirement for suitable supervision when students are using ICT equipment
- Ensure that there is a co-ordinated approach across the faculty/department to teaching internet safety issues. Staff have responsibility to remind all students of the risks and their responsibilities whenever ICT is used.
- Ensure that general discussion regarding internet safety matters and departmental/faculty compliance issues can take place at regular departmental/faculty meetings.

Behaviour Support Team

The Behaviour Support Team should:

- Monitor incidents of misuse regarding ICT e.g. Internet bullying
- Ensure that appropriate sanctions are applied and if a serious incident involving students that the incident is recorded and reported to the Internet Safety Co-ordinator should the police be required
- Be available if required to mediate for ICT-related incidents which occur outside the college eg bullying within chat rooms, the creation of hate websites aimed at individual students
- Not work in isolation regarding internet safety incidents – incidents must be logged and reported to the Internet Safety Co-ordinator in line with college policy. Knowledge of emerging issues should be shared with colleagues to increase awareness and to possibly pre-empt future problems.

Classroom Teacher and Teaching Assistants

Classroom teachers and Teaching Assistants and any adults working with children should:

- Develop and maintain knowledge of internet safety issues, particularly with regard to how they can affect children
- Implement college and departmental internet safety policies through effective classroom practice
- Ensure any instances of ICT misuse, whether accidental or deliberate, are dealt with through the proper procedures, reporting to the Behaviour Support Team in the first instance Internet Safety Co-ordinator
- Ensure that they provide the necessary support to students who experience problems when using the internet
- Plan classroom use of the internet and ICT facilities to ensure internet safety is not compromised

Inclusion Co-ordinator

The Inclusion Co-ordinator (DA) should:

- Develop and maintain knowledge of internet safety issues, particularly with regard to how they may affect students
- Develop and maintain additional policies and internet safety materials tailored to special educational needs of students
- Liaise with parents/carers of students with special educational needs to ensure they are aware of the internet safety issues their children may encounter outside college, and the ways they could support them.
- Co-operate with the Child Protection Liaison Officer as necessary
- Liaise with other individuals and organisations, as appropriate, to ensure that those students being educated away from college premises will benefit from a safe ICT learning environment.

Designated Safeguarding Officer

The DSO should:

- Seek professional development on safety issues relating to the use of internet and related technologies, and how these relate to students, refreshing this knowledge on a regular basis
- Liaise with the Internet Safety Co-ordinator on specific incidents of misuse
- Take a pro-active role in the internet safety education of students
- Develop systems and procedures for supporting and/or referring students referred to them as a result of breaches of internet safety within colleges
- Develop systems and procedures for students who self-refer, and those students identified as suspected 'victims' by teaching staff
- Develop relationships with colleagues and other organisations that can provide advice, resources and referrals relating to child protection on the internet.

LRC Support

Internet-accessible computers are positioned in view of the workstation. However, when a teacher brings a class of students into the LRC supervision and monitoring is the responsibility of the teacher.

It is advised that LRC support:

- Acts as a member of the college's internet safety team
- Develops an acceptable use policy for the LRC/BEC which is appropriate to the needs of the college and the library
- Provides input to the internet safety co-ordinator and the network manager on filtering issues, with reference to age and research activities of the students
- Advises on issues relating to information handling skills eg effective search skills, and information literacy as part of students' independent learning development
- Keeps informed of internet safety issues

Students

Students should be encouraged to take responsibility for their own actions when using the internet and other communications technologies. Students should develop confidence in their own abilities but should be able to recognise when it is appropriate to seek help and advice, and know where that can be found.

Students should:

- Contribute to college internet safety and acceptable use policies through involvement with the internet safety team
- Follow the college policies relating to acceptable use of the internet and other communications technologies
- Develop their own set of safe and discriminating behaviours to guide them whenever they are on line
- Report any incidents of ICT misuse within the college to a member of staff
- Seek help or advice if they experience problems on line, or if they receive any content or contact which makes them feel uncomfortable in any way
- Communicate with their parents/carers about internet safety issues

Section 5 - Internet safety in the Classroom

Education on internet safety is essential. The internet can provide many benefits but can also present very serious risks for those who are uninformed, unwary or unwise.

It is important that teachers, parent/carers and carers do not confuse skilful use of new technologies with an ability to perceive and avoid risk. Internet and ICT literacy does not indicate internet and ICT safety.

It has been found that students generally fall into one of three categories:

Group A - low level experience of the internet, prior exposure to internet safety advice and poor ICT skills. These will need guided learning with the teacher working more closely with the students and providing appropriate prompts.

Group B - moderate levels of experience of using the internet, moderate levels of prior exposure to internet safety advice and moderate ICT skills. This group is considered to have a moderate skill and knowledge base. They will benefit from resource-based learning to help them develop information literacy skills and independent learning skills.

Group C - high level of experience using the internet, high levels of prior exposure to internet safety advice and good ICT skills. They have a good skills and knowledge base and need to develop their abilities to reflect and apply their thinking to new situations. Knowledge of internet safety advice does not ensure that students will not engage in risky on-line behaviour. These students require just as much safety education as the other groups as this group is more likely to take risks.

Responding to Incidents of Misuse

1. Minor incidents of misuse by students include –
   - Copying information into essays and projects and failing to acknowledge the source (plagiarism and copyright infringement)
   - Downloading materials or images not relevant to their studies in breach of acceptable use policy
   - Misconduct associated with student logins eg using someone else's password
   - Incidents involving students using their own technology in college e.g. iPads, mobile phones being brought in and being used in class, sending nuisance text messages, unauthorised taking of images with mobile phone cameras, still or moving

If such an incident occurs
   1. It should be logged on the BfL system by the class teacher or other adult.
   2. The student issued with a warning in accordance with the Behaviour for Learning policy.
   3. Inappropriate technology should be confiscated and returned at the end of the day.
   4. If the behaviour escalates it should be responded to more seriously as the college then has evidence of previous events.
   5. The internet safety co-ordinator should monitor minor incidents by analysing the BfL log to identify trends in students' behaviour and react pro-actively to any emerging issues.
   6. The college internet safety policies should be reviewed regularly, especially the acceptable use policies.

2. More serious incidents involving inappropriate materials or activities –

   - Deliberately accessing, printing, showing or transmitting inappropriate (or age restricted) material within the college's network. Even if this was not deliberately accessed by the student, but not reported to the teacher and was subsequently shown to other students, this would also require a disciplinary response
   - Cheating in an examination or plagiarism in coursework which could also have legal implications regarding breach of copyright law.
   - Hacking or inducing a virus attack
   - Chronic truancy as a result of obsessive or excessive use of the internet and related technologies
   - Online gambling

Incidents involving one or more of the above are serious concerns and require an appropriate disciplinary response. If such an incident occurs;

1. It should be investigated by the Behaviour Support Team and details logged on the BfL system
2. Appropriate disciplinary action taken
3. The internet safety co-ordinator should be informed
4. The college internet safety policies should be reviewed regularly, especially the acceptable use policies.

3. Very serious incidents involving inappropriate materials or activities –

- It is illegal to show, give or sell restricted materials to a person under a certain age. Materials are classified to protect children from damaging their moral and physical wellbeing. Blatant, intentional exhibiting of age-restricted materials to students under the specified age is a serious breach of internet safety and requires strong disciplinary action.
- Any incident involving a member of staff is serious. It could have implications for the safety of the students, other staff and the learning environment, as well as the reputation of the college. It is vital an acceptable use policy is in place for staff and procedures are in place should incidents occur.
- Harassment of another person using ICT or a breach to their privacy poses a serious threat to their physical and emotional safety and again there may be legal consequences.

Incidents involving one or more of the above are very serious concerns and may be in breach of the law. These require an appropriate and immediate response. If such an incident occurs;

1. It should be investigated by the Internet Safety Coordinator or Headteacher/Child Protection Officer if ISC is not available.
2. The incident should be fully documented.
3. Appropriate action involving outside agencies should be taken, this may involve the Child Protection Officer and/or Head Teacher.
4. Incidents that involve inappropriate but legal material should be dealt with in college using the college's disciplinary procedures.
5. If a criminal offence has been committed and police involvement is required, then the Headteacher is advised to seek legal advice from the LA as soon as possible.
6. Any serious incidents may become the subject of media attention and it is important that the Headteacher is the contact for all media requests and that any ongoing investigations and the continuing safety of the college is not compromised.
7. The college internet safety policies should be reviewed asap, especially the acceptable use policies to prevent a recurrence.

4. Incidents involving illegal material or activities –

- The viewing, possession, making and distribution of indecent images of children
- Serious stalking or harassment facilitated by communication technologies

These offences could be committed by staff and students alike.

Incidents involving illegal activity require an appropriate and immediate response. If such an incident occurs;

1. Discovery of indecent material/activity of this nature within the college's network is a very serious situation and must always be reported to the police.
2. It is important that the material is not downloaded, printed or sent by e-mail as this will constitute an offence in itself.
3. If at all possible, nothing should be done to the suspect computer or computers, including turning them on or off.
4. It may be necessary to shut down the whole network but should only be done at the request of the police. Everyone should be kept away and nothing should be touched.
5. Under no circumstances should the internet safety co-ordinator, network manager or headteacher attempt to conduct an investigation of their own, or bring in an outside expert to do so as this may compromise evidence and may constitute an offence in itself in some cases.

6. In cases of student or staff involvement with indecent materials it would be advisable for the college to seek legal advice from the LA as soon as possible regarding disciplinary actions that are acceptable while the police carry out their investigations.
7. These incidents may become the subject of media attention and it is important that the Headteacher is the contact for all media requests and that any ongoing investigations and the continuing safety of the college is not compromised.
8. In the event of a very serious incident occurring within college it is essential to review all policies and procedures relating to internet safety as soon as possible. The three main components of a safe ICT learning environment ie the infrastructure of whole-college awareness, designated responsibilities, policies and procedures, the effective range of technological tools, and a comprehensive internet safety education programme must also be reviewed.

Section 6 - Working with Parents, Carers and the Community

1. Parents and carers must be aware that as well as the computer internet access many games consoles offer internet connectivity and they need to be aware of the potential hazards relating to these items.
2. Parent/carers must be aware of internet safety policies within college but also given practical strategies which could be adopted for the home.
3. The college must ensure through workshops or information exchange that parent/carers are supported regarding internet safety as many are discouraged by their lack of knowledge with computers.
4. Some parents/carers are unaware of the risks faced by the children when online and by education and support they will feel more able to guide and monitor their children's involvement with the Internet.

Section 7 - Acceptable Use of ICT Agreement

To ensure that all adult users of ICT facilities/equipment at the The City of Leicester College are fully aware of their responsibilities when using information systems, they are asked to read this agreement and sign to say that they have done so at the start of each year.

- I appreciate that ICT includes a wide range of systems, including iPads, mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for College business.

- I understand that the College uses software to monitor inappropriate or illegal use of ICT technologies which may result in screen shots from network computers being captured if they contain trigger words or phrases.

- I understand that sharing passwords may lead to breaches of security and I agree not to share any password or restricted usernames with anyone other than an authorized person.

- I will not destroy another user's files, create or introduce a virus to the College network.

- I recognize that information and software available via the network is subject to copyright and or restrictions on its use.

- I will not install any software or hardware without permission and will ensure license requirements are complied with fully.

- I understand that I have a legal responsibility to maintain the security of work related data and will ensure that personal data is stored securely (using a password at all times) and is used appropriately, whether in College, taken off the College premises or accessed remotely.

- I will respect copyright and intellectual property rights.

- I will ensure that electronic communications with pupils including email, Instant Messaging and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

- I acknowledge that all Data stored on the College network is the property of the College.

- I understand that I must inform the ICT Technical Department of accounts to be closed or data to be maintained and hardware to be handed in on departure from the College.

- I will use the ICT facilities responsibly and not waste College resources.

- I will ensure that students do not use College ICT equipment to play games for leisure purposes or send chain, junk or abusive or bulk emails.

- I will ensure that students leave the computers in a clean, usable state and report any faulty equipment to the ICT Technical Department.

- I will ensure that students do not eat or drink in computing rooms, labs or areas where ICT equipment is present.

- I will ensure that students do not disconnect machines or attempt to change the mice or keyboards and will not attempt to repair faults but will report all faults to the ICT Technical Department.

- I understand that it is a criminal offence to use College ICT systems for a purpose not permitted by its owner

The College may exercise its right to monitor the use of the College's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the College's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.