Launceston College

A Multi Academy Trust

E-SAFETY POLICY

Updated on: 21st June 2017

Review by: DAE

Launceston College eSafety policy

This e-safety policy has been developed by a committee made up of:

- School E-Safety Coordinator / Officer
- A member of ALT
- Teachers
- Support Staff
- ICT Technical staff
- Governors
- Parents and Carers
- Community users

Consultation with the whole school community has taken place through the following:

- Staff meetings
- School / Student / Pupil Council
- INSET Day
- Governors meeting / sub committee meeting
- Parents evening
- School website / newsletters

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the College Leadership Team*:*	
The implementation of this e-safety policy will be monitored by the:	*E-Safety Committee*
Monitoring will take place at regular intervals:	*Yearly*
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:	*To be included with Safeguarding briefing 3 times a year at Governors*
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:	
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*DAE , G Hockin, JAJ, ALT*

Scope of the Policy

This policy applies to all members of the Launceston College MAT community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of MAT ICT systems, both in and out of College.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the College.

The MAT will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of College.

Roles and Responsibilities

Governors:

The role of the E-Safety Governor will include:

- *regular meetings with the E-Safety Co-ordinator / Officer*
- *meetings with the E-Safety committee*
- *regular monitoring of e-safety incident logs*
- *regular monitoring of filtering / change control logs*
- *reporting to relevant Governors meetings*

The Academy Leadership Team:

- 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 E-Safety Co-ordinator.
- The Principal / Deputy Principals are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Principal / Deputy Principals will ensure that there is a system in place to allow for monitoring and support of those in College who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The Academy Leadership team will receive regular monitoring reports from the E-Safety Co-ordinator
- The Principal and another member of the Academy Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (See SWGfL flow chart on dealing with e-safety incidents – included later in this document)

E-Safety Coordinator / Officer:

The responsibilities of the E-Safety Coordinator are to:

- lead the e-safety committee
- take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the College e-safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provide training and advice for staff
- liaise with the Local Authority
- liaise with College ICT technical staff
- receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments, (Examples of suitable log sheets may be found in the SWGfL Safety and Security Booklet, along with the Internet Safety Protocol)
- meet regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attend relevant meeting of Governors
- report regularly to Academy Leadership Team

Network Manager / Technical staff:

The Network Manager / ICT Technical Team is responsible for ensuring:

- that the College's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the College meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the College's networks through a properly enforced password protection policy, in which passwords are regularly changed, (See School Password Security Policy)
- SWGfL is informed of issues relating to the filtering applied by the Grid
- the College's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in College policies

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 (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator for investigation / action / sanction
- digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official College systems
- e-safety issues are embedded in all aspects of the curriculum and other College activities
- students / pupils understand and follow the College e-safety and acceptable use policy
- they handle sensitive data in accordance with the College Personal Data Handling Policy
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended College activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current College policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils 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

Designated person for child protection / Child Protection Officer

should be trained in e-safety issues and be aware of the potential for serious child 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

E-Safety Committee

Members of the E-safety committee will assist the E-Safety Coordinator with:

- the production / review / monitoring of the College e-safety policy / documents.
- the production / review / monitoring of the College filtering policy

Students / pupils:

- are responsible for using the College ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to College systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand College policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand College policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of College and realise that the College's E-Safety Policy covers their actions out of school, if related to their membership of the College

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The College will therefore take every opportunity to help parents understand these issues through:

- newsletters, letters, website / VLE

Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy
- accessing the College website / VLE / on-line student / pupil records in accordance with the relevant College Acceptable Use Policy.

Community Users

Community Users who access College ICT systems / website / VLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to College systems.

Policy Statements

Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of students / pupils in e-safety is therefore an essential part of the College's e-safety provision. Children and young people need the help and support of the College to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in College and outside College
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students / pupils 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 / pupils should be helped to understand the need for the student / pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside College
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

The College will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, VLE
- Parents evenings

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- 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
- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at SWGfL / LA / other information / training sessions and by reviewing guidance documents released by SWGfL / LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training as required to individuals as required

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / SWGfL or other relevant organisation.
- Participation in College training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering 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:

- College ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of College ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted

- All users will have clearly defined access rights to College ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).
- All users will be provided with a username and password by the College ICT Technical Team who will keep an up to date record of users and their usernames.
- The “master / administrator” passwords for the College ICT system, used by ICT Technical Team must also be available to the Principal or another member of the College Leadership Team and will be stored in a secure location. (Currently a safe in the ICT Technical Team Office)
- Users are 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.
- The College maintains and supports the managed filtering service provided by SWGfL, In addition the College employs enhanced differential user-level filtering through the use of the ‘Censornet’
- In the event of the Network Manager (or other person) 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 E Safety Committee.
- Any filtering issues should be reported immediately to SWGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and ICT Technical Team, if the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee
- The ICT Technical team regularly monitor and record the activity of users on the College ICT 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 user’s activity.
- Users can report any actual / potential e-safety incident to the E-Safety coordinator or to a member of the ICT Technical Team.

- 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.
- An agreed policy is in place (to be described) for the provision of temporary access of “guests” (eg trainee teachers, visitors) onto the College system.
- An agreed policy is in place regarding the downloading of executable files by users, this in included as part of our student and staff acceptable use policy.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of College, this is included as part of our student and staff acceptable use policy.
- An agreed policy is in place that forbids staff from installing programmes on College workstations / portable devices.
- An agreed policy is in place (to be described) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on College workstations / portable devices. (see School Personal Data Policy Template in the appendix for further detail)
- The College infrastructure and individual workstations are protected by up to date virus software.
- Personal data can not be sent over the internet or taken off the College site unless safely encrypted or otherwise secured. (see School Personal Data Policy Template in the appendix for further detail)

Curriculum

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

- in lessons where internet use is pre-planned, it is best practice that students / pupils 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 / pupils are allowed to freely search the internet, eg 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 (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) 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 / pupils 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 / pupils 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 - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupil’s instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students / pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The College will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- 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 eg 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 / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the College into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students’ / Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs. (Unless express parental consent has been obtained)
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the College website, written permission is obtained in the form of a ‘Media Permissions Form’ which is part of the school admission pack. A central list is held of which students we are able to photograph is held in the Exams / Finance Office.
- Student’s / Pupil’s work can only be published with the permission of the student / pupil and 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.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with College policy (below) once it has been transferred or its use is complete

Communications

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

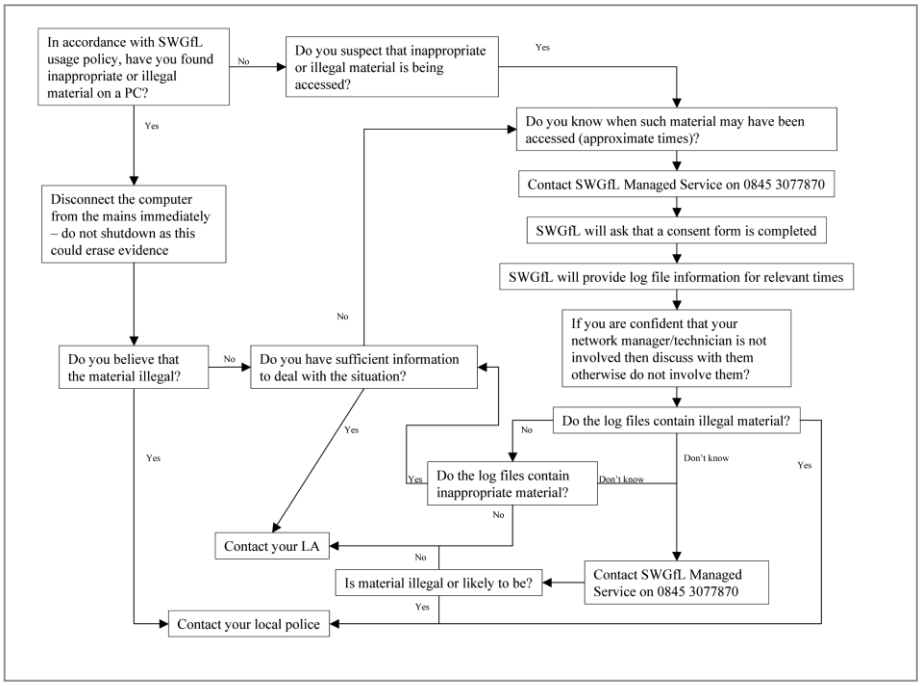
- The official College email service is regarded as safe and secure and is monitored. Staff and students / pupils should therefore use only the College email service to communicate with others when in College, or on College systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the E-Safety Co-ordinator or the ICT Technical Team – 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 / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) College systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the College website and only official email addresses should be used to identify members of staff.

Responding to incidents of misuse

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

the SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

It is more likely that the College will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the College community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.