EGGBUCKLAND
COMMUNITY COLLEGE

E-Safety Policy

THE PERFECT ENVIRONMENT
LEARNING | CARING | ACHIEVING

Eggbuckland Community College Academy Trust	
Policy:	E-safety Policy
Author:	Simon Crawford E-Safety Officer: Simon Crawford
Considered by Committee:	Curriculum and Pastoral Personnel (Jan 2016) FGB (March 2016) (March 2019)
Date Adopted:	March 2016 (Following E-Safety Review – July to Dec 2015)
Next Review:	March 2022

This policy is in line with:

- Sections 175 and 157 of the Education Act 2002, implemented June 2004.

- Working Together to Safeguard Children (March 2015).
- What To Do If You Are Worried A Child is Being Abused; Advice for Practioners (March 2015).
- Keeping Children Safe in Education (March 2015)
- ECC Safeguarding Policy
- South West Grid for Learning '360 degree safe' Self Review Process

Linked Policies

- Preventing Extremism and Radicalisation
- Behaviour for Learning (inc. Anti-bullying)
- Child Protection and Safeguarding
- Health and Safety
- Anti-Discrimination
- Anti-Bullying
- ICT Acceptable Use Policy
- Data Protection Policy
- Whistleblowing Policy

Key information from this Policy is displayed in the staffroom and is available in the staff handbook.

Rationale

E-safety comprises all aspects relating to children and young people and their safe use of the internet, mobile phones and other technologies, both in and out of College. It highlights the need to educate children, young people, parents, staff and all members of the College community about the benefits, risks and responsibilities of using information technology and provides safeguards and awareness for users to enable them to control their online experiences.

The internet is an open communications channel, available to all. Applications such as the Web, e-mail, blogs and social networking all transmit information over the fibres of the internet to many locations in the world at low cost. Anyone can send messages, discuss ideas and publish material with little restriction.

These features of the internet make it an invaluable resource used by millions of people every day. Much of the material on the internet is published for an adult audience and some is unsuitable for students. Students must also learn not to publish personal information.

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

Principals are empowered, to such extent as is reasonable, to regulate the behaviour of students when they are off the College site. This is pertinent to incidents of cyber-bullying, or other E-safety incidents covered by this policy, which may take place out of College, but are linked to membership of the College.

The College 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.

Contents

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / students to take a responsible approach. The education of students / students 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 education will be provided as part of P4L, the assembly programme, visiting speakers and ICT curriculum - this will cover both the use of ICT and new technologies in College and outside College.

- 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 will be helped to understand the need for the Student Code of Conduct for ICT and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside College. This includes usage in the classroom under Bring Your Own Device (BYOD) arrangements.

- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Education – Parents and 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 and regulation of the children's online 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.

"There is a generational digital divide". (Byron Report - 2010)

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

- Letters, newsletters and the College website.
- E-safety parents' evenings.
- Reference to the SWGfL Safe Website and CEOP.

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:

- E-safety training will be provided annually to all staff, who will be asked to sign to say they have read the document.

- 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 Code of Conduct for ICT.

- Staff who are new to the College or who are provided with new devices or passwords, will be asked to sign/re-sign the Colleges ICT acceptable Use Policy.

- The E-safety Officer will receive regular updates through attendance at SWGfL and LA training sessions and by reviewing guidance documents released by BECTA, SWGfL , CEOP, the LA, the DfE and others.

- This E-safety Policy and its updates will be presented to and discussed by staff in staff meetings.

- The E-safety Officer will provide advice / guidance / training as required individuals as required.

Training – Governors

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

- Participation in College training events.

- Attendance at training provided by the National Governors Association, SWGfL or other relevant organisation.

Roles and Responsibilities

The following section outlines the roles and responsibilities for E-safety of individuals and groups within the College:

Governors

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 / Governors Sub Committee receiving regular information about E-safety incidents and monitoring reports.

A member of the Governing Body has taken on the role of E-safety Governor.

The role of the E-safety Governor will include:

- Regular meetings with the E-safety Officer
- Regular monitoring of E-safety incident logs
- Regular monitoring of filtering logs
- Reporting to relevant Governors committee

Principal and Senior Leaders

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 Officer.

The Principal / Senior Leaders are responsible for ensuring that the E-safety Officer 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 / Senior Leaders 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.

The Principal and E-safety Officer 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.

E-safety Officer

Takes day -to-day responsibility for E-safety issues and has a leading role in establishing and reviewing the College E-safety policies / documents. The role

includes:

- 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 the Local Authority, when needed.

- Liaises with College ICT technical staff.

- Receives reports of E-safety incidents and creates a log of incidents to inform future E-safety developments.

- Meets regularly with the E-safety Governor to discuss current issues, review incident logs and filtering logs.

- Attends relevant meeting / committee of Governors.

- Reports regularly to Senior Leadership Team.

- Authorises investigations into the use of ICT within the College. This Includes Internet usage with particular reference to 'User Actions' (see Page 17).

Network Manager

The Network Manager 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

- 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

- That he / she keeps 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 / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-safety Officer /Principal / Senior Leader / Class teacher / PL for investigation / action / sanction

- That monitoring software / systems are implemented and updated as agreed in College policies

Teaching and Support Staff

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 Acceptable Use Form for ICT
- They report any suspected misuse or problem to the E-safety Officer, Principal, Senior Leader, Class teacher, PL for investigation and action
- Digital communications with students should be on a professional level and only carried out using official College systems. Staff should also be mindful of appropriate timing and context of all direct communication with students.
- E-safety issues are embedded in all aspects of the curriculum and other College activities
- Students understand and follow the College E-safety policy
- Students 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, media devices, 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 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
- Staff should be mindful that their 'duty of care' extends to ex-students. Due diligence should be taken with regard to safeguarding in relation to communications or otherwise, with these people.

Child Protection Officers

The Child Protection Officers 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
- Sexting
- Potential or actual incidents of grooming / Child Sexual Exploitation
- Cyber-bullying

It is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.

Students

Students are responsible:

- For using the College ICT systems in accordance with the ICT Permission Form and Rules (in student planners), which they will be expected to sign before being given access to College systems.

- For having a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- For understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

- For knowing 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.

- For understanding 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 College, if related to their membership of the College

Parents and Carers

Parents and 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 parents' evenings, newsletters, letters, the College website and information about national E-safety campaigns / literature.

Parents and carers will be responsible for:

- Endorsing (by signature) the ICT Permission and Rules Form (in student planners).

- Alerting the College straight away if they have any E-safety concerns or require advice/guidance.

Community Users

Community Users who access College ICT systems College will be expected to sign

a Staff Acceptable Use Form before being provided with access to College systems.

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 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.

- There will be regular reviews and audits of the safety and security of College ICT systems.

- Servers, and wireless systems must be securely located and physical access restricted.

- All users will have clearly defined access rights to College ICT systems.

- The Network Manager, who will keep an up to date record of users and their usernames, will provide all users with a username and password. Users will be requested to change their passwords regularly.

- The "administrator" passwords for the College ICT system, used by the Network Manager must also be available to the Principal and E-safety Officer 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.

- The College maintains and supports the managed filtering service provided by Sophos UtM.

- In the event of the Network Manager 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 Principal or E-safety Officer.

- Any filtering issues should be reported immediately to the Network Manager.

- College ICT technical staff 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 for ICT.

- Remote management tools are used by staff to control workstations and view student activity.

- Users must report any actual / potential E-safety incident to the Network Manager or E-safety Officer.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, hand held devices etc from accidental or malicious attempts which might threaten the security of the College systems and data.

- The College infrastructure and individual workstations are protected by up to date virus software.

- Personal data cannot be sent over the internet or taken off the College site unless safely encrypted or otherwise secured.

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 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, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager 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

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students 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. Eggbuckland Community 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 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 where possible. Ideally 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.

Written permission from parents or carers (through the Admissions Form) will be obtained before photographs of students are published on the College website.

Students' work can only be published with the permission of the student and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 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.

We strongly recommend that staff do not use them however, 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 once it has been transferred or its use is complete.

Communication

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

- The official College email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the College email service to communicate with others when in College, or on College systems (e.g. by remote access).

- Users need to be aware that email communications may be monitored.

- All staff must adhere to the Email Protocol.

- Users must immediately report, to the Principal, E-safety Officer or Network 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 must be professional in tone and content. These communications should 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.

- Personal information should not be posted on the College website and only official email addresses should be used for communication.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of students, the College and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards'.

All Colleges, academies and local authorities have a duty of care to provide a safe learning environment for students and staff. Colleges/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render Eggbuckland Community College liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The College provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the College through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings;

data protection; reporting issues.

- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.
- College staff should ensure that:

- No reference should be made in social media to students / students' parents / carers or College staff.

- They do not engage in online discussion on personal matters relating to members of the College community.

- Personal opinions should not be attributed to the College /academy or local authority.

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist or extremist material is illegal and would obviously be banned from Eggbuckland Community College and all other technical systems.

Other activities e.g. cyber-bullying are also banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a College context, either because of the age of the users or the nature of those activities.

The College policy both restricts and encourages usage as outlined on the next page.

User Actions		Acceptable for users	Acceptable in Most Circumstances(see note)*	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978				X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.				X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008				X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986				X
	pornography			X	
that contain or relate to:	promotion of any kind of discrimination (including racial, sexual, political, or religious)			X	
	threatening behaviour, including promotion of physical violence or mental harm			X	
	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			X	
Using College systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the College / academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			

NB These are examples only – other circumstances apply.

On-line gaming (non educational)		X			
On-line gambling		x			
On-line shopping / commerce			X		
File sharing				X	
Use of social media(private and personal) during working hours					X
Use of messaging apps				X	
Use of video broadcasting eg Youtube			X		

**The College seeks to promote the full and effective use of technology and requires that staff take portable devices home with them. The use of these devices is not, and should not be, restricted to College matters. Examples of home use could include internet banking, viewing films, internet shopping etc. Unacceptable and illegal activities defined above remain forbidden.*

Student E-safety incident procedures

Out-of-College cyber-bullying incident

1. PL and Pastoral Support Staff to investigate incident.
2. Students involved to be spoken to.
3. Parents informed.
4. Appropriate sanctions issued.
5. Pastoral Support Staff to provide support, advice and guidance

In-College cyber-bullying incident (involving College network or mobile devices)

1. PL and Pastoral Support Staff to investigate incident.
2. Pastoral Support Staff to contact Network Manager to have network access removed of students using the College system to cyber-bully.
3. Parents informed.
4. Appropriate sanctions issued.
5. Pastoral Support Staff to provide support, advice and guidance.

Accessing another person's network account without permission

1. If the incident happens within a lesson the responsibility for taking action lies with the subject teacher.
2. If the incident occurs outside of lesson time the PL will take responsibility.
3. In both circumstances the Network Manager should be contacted and network access removed for a fixed period.
4. Appropriate sanctions issued.

5. Parents to be informed.

Accessing inappropriate/illegal material or bringing such material into College

1. If this involves the use of the College network please contact the Network Manager immediately to ensure the user account is frozen to avoid deletion.
2. Referral to the appropriate PL who will then investigate.
3. Appropriate sanctions issued (including exclusion if necessary) and network access removed for a fixed period.
4. Parents to be informed.
5. Pastoral Support Staff to work with student(s) so that they realise that accessing such material is not appropriate.

In the event of several E-safety incidents involving the same student(s) then referral to the E-safety officer is appropriate.

On-line child protection concerns

1. Immediate referral to a Child Protection Officer in-line with CP procedures.
2. CPO to coordinate response including possible Police and Social Services involvement.

Staff E-safety incident procedures

All suspected incidents of staff e-safety procedures shall be dealt with by the E-safety Officer in the first instance.

Any incident of a breach of E-safety procedures could result in disciplinary action.

If there is any suspicion of an E-safety matter that involves illegal activity or safeguarding, they will be immediately reported to the College Child Protection Officer and the Principal.

SWgfL have strict filters in place and will inform the Police automatically if the College internet is used for any illegal activity involving safeguarding.

Staff should be mindful that they should not engage in activity online, including at home, that could potentially compromise their professional standards.