Jersey College for Girls

Online Safety Policy November 2016

Authors:	Emma Silvestri-Fox (Designated Safeguarding Lead) Ruth Lea (eSafety Officer)

Agreed by Staff:	November 2016
Agreed by Governors:	January 2017
To be reviewed:	November 2018

Introduction:

The internet and constantly evolving technology continually changes the way that we all interact with the world. Whilst advances in technology offer a plethora of excellent opportunities for teaching and learning this technology comes with some potential risks.

Online safety is not purely about technology. Many of the issues arising from online activity are behavioural and consequently will be managed in the same way as any other inappropriate behaviour.

E-Safety messages such as 'don't post personal information online' are now almost meaningless, as the whole point of social media for many young people is to share personal information. Also the huge range of online applications now used means that locking information down via privacy settings is almost impossible.

Our key aim with respect to the use of technology is that there is no substitute for a strong established culture of safeguarding within the College, which prioritises the safety of both our students and staff, especially in relation to the use of online apps, social media and wireless technology.

Objectives:

To achieve these aims our policies, systems and procedures are designed to:

- help students and staff to identify and manage risks when using technology.
- use filtering and monitoring technologies to prevent students and members of staff from gaining either accidental or deliberate access to unacceptable online content whilst on the College's premises or using College facilities.
- encourage students and staff to report anything they encounter online which concerns them.
- ensure, wherever possible, that students and staff do not engage in inappropriate activities when using technology whilst at school.
- encourage students and staff to communicate appropriately, for example using only school email addresses to communicate with students.

- regularly inform students, parents and staff about the latest potential online risks and concerns, also alerting them to related matters that include, online reputation, data protection and identity theft.

Systems and Procedures:

Staff:

1. have a responsibility to familiarise themselves with the most up to date Education Online Safety policy and procedures documentation (see appendix 1)

2. are required to sign the JCG Staff Acceptable Use Agreement (see appendix 3) and the JCG Child Protection Policy

3. have a responsibility to follow the College Safeguarding reporting procedure and it is essential that any information or concerns regarding eSafety are communicated as soon as is reasonably possible to the Designated Safeguarding Lead. (See College Child Protection Policy)

4. should be aware of online eSafety procedures and positively communicate the importance of maintaining Digital Safeguarding in the use of technology with their students

5. should, when using social networking sites for their private use ensure that their privacy settings are appropriate, protecting their online reputation and they should not, for example, befriend students, and also be aware of potential risks associated with befriending ex-students

6. have a responsibility to ensure that any online information, in either a personal or professional capacity, protects their professional integrity and does not bring their self, the College, the States of Jersey nor the teaching profession into disrepute
7. should, when selecting websites/ online content for learning, review it to use with students, check their Terms & Conditions with regard to data protection compliance and the minimum age set for the websites to protect children from risk of harm or to comply with legal requirements
8. should participate in appropriate eSafety and child protection training when requested

9. should keep themselves informed of current online eSafety issues
10. have a responsibility to teach and support students to identify and manage risks associated with online behaviour and reputation
11. have a responsibility to maintain and keep data secure, ensuring all sensitive data is stored on the Q (sensitive) network drive and is appropriately encrypted

12. should never allow their network log-in to be used by a student

13. who wish to use social networking sites for educational purposes must complete an appropriate risk assessment and have approval from the eSafety officer.

Online Safety Training for Staff:

1. All new staff will be given guidelines and procedures during their induction period.

2. The College will provide appropriate eSafety training.

3. NQTs will receive training from the Education department as part of their induction programme.

4. Where appropriate, individual staff may access further relevant training.

The eSafety Officer and the DSL have joint responsibility for:

1. having a clear understanding of child protection, eSafety and data protection policies and procedures – and be able to determine the applicable policies/ procedures for different situations
2. acquiring appropriate relevant training regarding new technologies and their impact on Online Safety

3. attending eSafety / Online Safety conferences and strategy meetings

4. identifying training needs for the Student Support Team

5. being the primary point of contact between the College and the Education departments Head of Governance (Mel Pardoe)

6. planning and delivering student and parent awareness programmes (e.g. information booklets, parent information evenings)

7. sharing and evaluating concerns held by staff so that appropriate action to safeguard the welfare of students can be taken
8. ensuring members of staff are informed about lines of external support that are available to them, such as the Professionals' Online Safety Helpline (helpline@saferinternet.org.uk) operated by the UK Safer Internet Centre http://www.saferinternet.org.uk/about
9. monitoring and responding to Lightspeed (filtering) and Impero (monitoring software) alerts as appropriate
10. ensuring eSafety / Online Safety signage and information is visible around the College and is regularly updated
11. supporting students who may be the subject of any Online Safety concerns and referring to outside agencies if appropriate

12. liaising with and supporting staff who have concerns about Online Safety

13. maintaining confidential records of meetings and events relating to Online Safety issues

14. making use of the 360 degree safe school self-review tools to inform the College Online Safety Policy
15. maintaining a record of staff who are using social media with their students and ensuring that risk assessments where appropriate are updated for websites and Apps

All Students should be encouraged to take responsibility for:

1. their own online eSafety and, together with parents, sign and abide by the student AUA (Appendix 2)
2. ensuring that their Online Profile is secure and does not make them vulnerable
3. respecting personal privacy and keeping their own and other people's personal information private, including photographs, passwords and any staff mobile phone numbers given out for the purposes of a school trip.
4. realising that the need to respect each other is equally important online as it is face to face contacts
5. reporting inappropriate use of technology immediately to a teacher
6. engaging in lessons on eSafety awareness and Online Safety training
7. behaving in a healthy and positive manner towards digital technologies and when engaging in online activities

Parents/guardians have responsibility for:

1. discussing and supporting their child abide by the AUA (Appendix 2)
2. discussing the need to be safe online with their child
3. encouraging their daughters to report any concerns regarding online safety to them or to the school
4. accessing support systems in school and via the Internet to develop an appropriate awareness of how to protect their child
5. Contacting the College (eSsafety Co-ordinator or DSL) with any concerns regarding Online Safety
6. respecting data protection issues when sharing images, videos and text, especially personal information about their child on social media networking sites
7. respecting school passwords and encouraging their child never to attempt to obtain or to use another child's or an adult's password
8. encouraging their child to read and respect (or to ask for advice or permission as appropriate) the Terms & Conditions of web services, especially with regard to the minimum age that some companies set for their websites in order to protect children from risk of harm or to comply with legal requirements

The Principal has responsibility for:

1. overseeing the application of the Online Safety Policy
2. supporting the eSafety Officer as appropriate.
3. ensuring that a member of the SLT team assumes the responsibility of the eSafety officer should the DSL or the designated eSafety Officer be absent.

Relationships to other policies

External policies to be found at:
http://www.gov.je/Government/Departments/EducationSportCulture/Pages/Policies.aspx#anchor-4

1. Child Protection (ED)
2. Online Safety Policy for Schools and Youth Projects (ED)
3. Health and Safety (ED)
4. Data Protection (ED)

Internal Policies:
To be found at: T drive College network

1. Child Protection
2. Improving Behaviour Policy
3. Counter bullying policy

Student Acceptable Use Agreement
Staff Acceptable Use Agreement

Appendix 1

Education Department Online Safety Policy

http://www.gov.je/SiteCollectionDocuments/Education/P%20Online%20Safety%20Policy%2020160915%20MP.pdf

Appendix 2

Acceptable Use Agreement (AUA) for use of technology in College

We would like to give every JCG student and member of staff the opportunity to use up to date technology to support learning at the College. We believe that technology and the Internet provide many opportunities for learning, communication, creativity and freedom of expression. However, with advances in technology comes responsibility and a need for maturity. It is essential that all students respect the privacy of others and protect their own online reputation and are aware that inappropriate use of technology can cause distress and harm to others, and lead to anti-social behaviour.

This is why we would like you to read and agree to the following Acceptable Use Agreement; to protect and limit the likelihood of harmful incidents to you and others, to help you make informed decisions and to take responsibility for your online 'life'.

When using a mobile device in school we would encourage staff and students to connect to the College filtered wireless network to access the Internet rather than opting for the unfiltered and costly 3G/4G networks. Using the College network will help us protect you from inappropriate and potentially distressing content. Please, help us to keep you safe online by registering your device for use on the College wireless network. To register a device you will need to take your device to the AVA office.

When using the school network, personal mobile technology in school and Office365 I agree to the following AUA:

- I know that the College networks are monitored and by connecting to the networks I give consent for this monitoring to take place.
- I will password/passcode my device.
- I will not share my username and passwords with other users.
- I will not use messaging Apps during lesson time (unless student is instructed by teacher).
- I will not use Social Media or Messaging Apps to cause hurt or embarrassment to another person.
- I will not take photos or video/audio recordings of another person without their permission.
- I will not take photos or video/audio recordings of others with the intention to cause hurt or embarrassment.
- I will not post/publish/upload to Office365 OneDrive images or video/audio recordings of other people on the Internet (unless student is instructed by teacher),
- If I see a message, comment, image, or anything else online that makes me concerned for my personal safety or that of others I will **report it immediately to the school[1].**
- If I see a message, comment, image, or anything else online that causes hurt or embarrassment to a student, member of staff at JCG or someone known to me I will **report it immediately to the school[1]**.

[1]Form tutor, subject teacher, the Designated Safeguarding Lead (Mrs Silvestri-Fox), Principal (Mr Howarth).

- I understand that bullying whether online or other will not be tolerated and is strictly forbidden.
- I will not store any personal school based data on web-based (cloud) services (e.g. iCloud and GoogleDrive) that are hosted outside Jersey unless permitted by the school and agreed by the Jersey Data Protection Commissioner.
- I understand that devices bought into school are done so at the owner's own risk,
- Where possible I agree to have up-to-date anti-virus and other security software (such as privacy protection applications) installed on my device.
- I understand that the on-site use of my mobile device is a privilege for students, not an automatic right and may be withdrawn if misused.
- As a **student** I grant the College a right of inspection of my device when there is a cause for concern. All inspections will be carried-out only by designated members of staff[2]. I am entitled to insist that a parent/guardian is present throughout any inspection. If I refuse an inspection request I may be refused permission to use my device in school. In cases of serious concern, a refusal may result in the involvement of external agencies including the police.

[2]designated staff are the Designated Safeguarding Lead (Mrs Silvestri-Fox), Vice Principal (Miss Rollo) and the Principal (Mr Howarth).

Withdrawal of consent

Contravening the terms of this agreement may result in withdrawal of consent to use the school network and, in extreme cases, disciplinary action and/or the involvement of third-party agencies.

I confirm that I have read through the agreement with my parent/guardian and agree to adhere to the principles outlined in the AUA.

Name of student: ***Tutor Group:***

Signature: …….. ***Signature: ……..*** ***Date:…….***
Parent/Guardian Student

Please return to the College office.

Appendix 3

JCG Staff Acceptable Use Agreement (AUA) for use of Technology in College

Introduction

We would like to give every JCG student and member of staff the opportunity to use up to date technology to support learning at the College. We believe that technology and the Internet provide many opportunities for learning, communication, creativity and freedom of expression. However, with advances in technology comes responsibility. It is essential that all members of JCG respect the privacy of others and protect their own online reputation and are aware that inappropriate use of technology can cause distress and harm to others, and lead to anti-social behaviour. We have asked all students to sign a similar AUA.

This is why we would like you to read and agree to the following Acceptable Use Agreement; to protect and limit the likelihood of harmful incidents to you and others and to help you make informed decisions.
Please do not view the AUA as a list of dos and don'ts, but a necessary agreement to protect you and the students in your care. In our ever changing 'Tech World', it is very easy to innocently use technology/Apps which may have potential data protection and eSafety issues.

When using a mobile device in school we would encourage staff (and students) to connect to the College filtered wireless network to access the Internet rather than opting for the unfiltered and costly 3G/4G networks. Using the College network will help us protect you from inappropriate and potentially distressing content – essential if the device is used for teaching. Please, help us to keep you safe online by registering your device for use on the College wireless network. To register your device you will need to take the device to the AVA office.

The Acceptable Use Agreement

When using the school network, school owned devices, personal mobile technology* in school and Office365 I agree to the following AUA: ** smart phone, ipad, tablet, laptop*

- I know that the College networks are monitored and by connecting to the networks I give consent for this monitoring to take place.
- I will password/passcode my device and not share with other users.
- I will not share my network username and passwords with other users.
- I will only use messaging Apps and Social Media during the school day exclusively for teaching and learning purposes.
- I will not use Social Media, Messaging Apps, photo/video/audio Apps to cause hurt or embarrassment to another person or in any way which brings my professionalism into question.

- I will not take photos or video/audio recordings of another person without their permission and am aware of which parents/ guardians have not given permission for their child to be photographed *(T:\Admin\Student\Student photos, media etc – EXCEPTIONS)*
- I will preview any online video before using it for teaching and learning, especially if the source is YouTube and take the necessary precautions.
- I will not use technology for personal use during contact time.
- I will not post/publish/upload to Office365 OneDrive images or video/audio recordings of other people on the Internet without first referring to of parental/guardian permission information
- If I see a message, comment, image, or anything else online that makes me concerned for my personal safety or that of others I will **report it immediately to either ESF[1] or Heads of Key-Stage**
- If I see a message, comment, image, or anything else online that causes hurt or embarrassment to a student, member of staff at JCG or someone known to me I will **report it immediately to either** Designated Safeguarding Lead [1] or Heads of Key-Stage

  [1] *The Designated Safeguarding Lead (Mrs Silvestri-Fox)*
- I understand that bullying whether online or other will not be tolerated and is strictly forbidden and I will act responsibly and with immediacy to protect those in my care.
- I will not store any personal school based data on web-based (cloud) services (e.g. iCloud and GoogleDrive) that are hosted outside Jersey unless permitted by the school and agreed by the Jersey Data Protection Commissioner. (Office365 is permitted)
- I agree to store all sensitive data in the Q drive on the College Network
- Know the definition of sensitive data
- I will not store any sensitive data on Office365
- I understand that before using any Apps for teaching and learning, beyond the school agreed Apps, I am required to write a risk assessment and have agreement from either Education or the College eSafety officer before use (*eSafety Officer (Miss R Lea))*
- I agree to attend eSaftey training offered by the College or read documentation when requested to raise my awareness of the latest eSafety issues.
- I understand that devices brought into school are done so at the owner's own risk and should not contain any data which has the potential to bring harm or embarrassment to myself or others or bring the College reputation into disrepute.
- Where possible I agree to install up-to-date anti-virus and other security software (such as privacy protection applications) on my device.
- I understand that in signing the College loan agreement I am responsible for the security and data stored on the device. (If the device requires repair due to negligence/misuse within 3 years of its purchase, I expect to pay the cost for the full repair.)
- I understand that if there is serious concern about the data stored on my personal or loaned devices external agencies including the police will be contacted.

Withdrawal of consent

Contravening the terms of this agreement may result in withdrawal of consent to use the school network and, in extreme cases, disciplinary action and/or the involvement of third-party agencies.

I confirm that I have read through the agreement and agree to adhere to the principles outlined in the AUA.

Name:

Signature: ..... *Date:.....*

Please return to the College office by Friday 18 Nov 2016