Policy name	Online safety policy for Crimson Global Academy		
Policy number	CS -07		
Review cycle	Every year		
Reviewed	2022.2.14	Next review	2023.2.14

Introduction

It is the duty of Crimson Global Academy (CGA) to ensure, as far as possible, the online safety of all the students who attend the School.

Aims of the policy

The aims of this policy are to identify risks that may face members of the School and how the School will work to minimize those risks where possible. This policy document will apply to all members of the School; students, teachers, support staff and volunteers who have access to the school's IT platforms.

Scope of the policy

This policy applies to all members of the School community who have access to the School's IT systems, including staff, students, volunteers and parents.

In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes students' carers.

This Policy covers both fixed and mobile internet devices (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment etc.).

This policy document is to be read in conjunction with:

(i) the school rules documentation regarding online action of CGA students – **see appendix 1** ; and
(ii) the Acceptable use of Technology policy – **see appendix 2**

Roles and responsibilities

1. **The Board of Governors**

   The governing body of the School is responsible for the approval of this policy and for reviewing its effectiveness. It will review this policy every year.

   The nominated governor for safeguarding takes responsibility for ensuring that the E-Safety Policy is implemented.

2. **The Executive Principal, the Principal and the SMT, including the Deans**

   The Principal is responsible for the safety of all the members of the School community, and this includes responsibility for E-Safety.

   The Principal has delegated day-to-day responsibility to the Head of E-Safety. In particular, the role of the Executive Principal, the Principal and SMT is to ensure that:

   a. staff, in particular the E-Safety Coordinator, are adequately trained about E-Safety; and
   b. staff are aware of the School procedures and policies that should be followed in the event of the abuse or suspected breach of E-Safety in connection to the School.

3. **E-Safety Coordinator**

   The School's E-Safety Coordinator is responsible for the day-to-day issues relating to E-Safety. The E-Safety Coordinator has responsibility for ensuring this policy is upheld by all members of the School community and works with IT staff to achieve this. The post-holder will keep up to date on current E-Safety issues and guidance issued by relevant organisations, including NetSafe NZ.

4. **Technical staff**

   The School's technical staff have a key role in maintaining a safe technical infrastructure at the School and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the School's hardware system and its data. They provide appropriate access to, and monitor the use of, the internet and emails; they maintain content filters and report inappropriate usage to the E-Safety Coordinator.

5. **Staff**

   Anyone accessing the School’s IT infrastructure is required to abide by the Acceptable Use Policy. **See appendix 2**

All staff working with Students are responsible for demonstrating, promoting and supporting safe behaviours in their lessons and following school E-Safety procedures. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any E-Safety issues which may arise on a daily basis.

Staff have a responsibility to record and report any incidents or concerns relating to E-Safety using a Safeguarding Note of Concern, which they should pass on as soon as possible to the School's Designated Safeguarding Lead (DSL):

E-Safety reporting form

6. **Students**

All Students are required to abide by the **Acceptable Use Policy – Appendix 2** - when accessing the School's IT infrastructure, and must let staff know if they see IT systems being misused.

7. **Parents and carers**

Parents and carers are responsible for endorsing the School's Acceptable Use Policy, and for promoting E-Safety, both in and outside of school.

Education and training

1. **Staff: awareness and training**

New staff receive information on CGA's E-Safety and Acceptable Use Policies as part of their induction.

Staff are made aware of their individual responsibilities relating to the safeguarding of children within the context of E-Safety. They also receive, as and when appropriate, additional guidance and training on E-Safety issues.

Onboarding teachers' tutorial slides - declare that the slides have been watched as part of Sapling onboarding process.

On going training - changes in policy will be provided by the E-safety coordinator at weekly meetings.

Termly HoD meetings in Auckland discuss any changes in the E-safety, which will be passed onto staff in departmental meetings and school meetings.

The rapid and constant evolution of the digital environment will be continually evaluated by the E-Safety Coordinator and relayed to staff at appropriate times during the year.

2. **Students : E-Safety in the curriculum**

The majority of the E-Safety curricular will be covered in the Form periods by the form teachers.

A curriculum of e-safety, produced by the E-Safety coordinator, will be presented to the full time students. This will include:

a. An introduction to NETSAFE (Southern Hemisphere Schools)
b. An introduction to ChildNET (Northern Hemisphere Schools)

The curriculum will be visible on the school's website.

3. **Parents**

The School seeks to work closely with parents and carers in promoting a culture of E-Safety. This will be supported by the appropriate help and training material for parents and caregivers on the school website.

The School will always contact parents if it has any concerns about Students' behaviour in this area, and likewise it hopes that parents will feel able to share any concerns with the School.

Use of internet and email

Staff

All digital communication between staff and students must take place using school accounts on CGA email, Slack or CANVAS messenger. **Staff are expressly forbidden from having contact with Students via private email or social media accounts.**

The School has taken all reasonable steps to ensure that the School network is safe and secure. Staff should be aware that all activity on the School's network, including email communication via staff email addresses, is monitored.

Communication, via email, Zoom or Whereby, between staff and students or parents/carers must be professional in tone and content.

When using school systems, staff should immediately report to the E-Safety Coordinator or DSL any online material or email communication which makes them feel uncomfortable, or is offensive, discriminatory, threatening or bullying in nature. **They must not respond to any such communication**.

Staff must remain alert to the risk of fraudulent emails. They should report emails they suspect to be fraudulent to the E-Safety Coordinator, DSL or the Head of the Technology Services Department, Guy Sherman.

Students

All students are issued with their own personal school email addresses and usernames for use on our network. Access is via a personal login, which is password protected. This official service may be regarded as safe and secure and must be used when submitting schoolwork electronically. Students should be aware that email communications through the School network and school email addresses are monitored.

There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system.

Students must only use their school accounts to email staff; they must not seek to contact staff via private email or social media accounts.

Students must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature, and should immediately report such a communication to a member of staff, preferably their Dean or DSL.

The School expects students to think carefully before they post any information online, or re-post or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Students must report any accidental access to materials of a violent or sexual nature directly to their Dean as soon as possible. They must **not** forward the material to the Dean but should forward it to the police in their country of residence if the School feels the severity of the material warrants it.

Password security

Students and staff have individual Learning Management System accounts, email addresses and Google logins and passwords.

Staff and students should be regularly reminded of the need for password security.

All staff and students should:

a. use a strong, unique password consisting of at least 14 characters. This should include a mixture of capital and lowercase letters, numerals and special characters. It must not include a group of three characters from the username.
b. never share their passwords.

Safe use of digital and video images – see the rules and regulation of CGA – **Appendix 1**

Staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform students about the risks associated with their creation, use, sharing, publication and distribution. In particular, they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

Parents/carers are permitted to take videos and digital images of their own children at school events for their own personal use, provided that they have the permission of the member of staff responsible for the event.

To respect everyone's privacy and, in some cases, protection, these images must not be published (e.g. on blogs or social networking sites) without the permission of the people identifiable in them.

Staff are allowed to take digital/video images to support educational aims.

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 School into disrepute.

Students must not take, use, share, publish or distribute images of others, except when in connection with a clear educational purpose and/or authorised to do so by staff.

Photographs published on the School website, or displayed elsewhere, which include students, will be selected carefully and will comply with good practice guidance on the use of such images. When photographs are to be published accompanied by the full names of Students, permission from parents/carers will be obtained. (See the **Parent Contract** and **Acceptable Use Policy – appendix 2 of this document** for more information.)

Misuse

CGA will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police in the relevant country of residence of the person concerned.

Incidents of misuse or suspected misuse will be dealt with by staff in accordance with the School's policies and procedures (in particular the Child Protection Policy and the Behaviour, Rewards and Sanctions documents).

Complaints

As with any issues that may present themselves at CGA, if a member of staff, a student or a parent/carer has a complaint or concern relating to E-Safety, prompt action will be taken to deal with it.

Complaints should be addressed to:

1. Child safety, the DSL – Mr. Mark Phillips - m.phillips@cga.school.nz

2. Technical issues, the Head of Crimson Technology Department – Guy Sherman - g.sherman@crimsoneducation.org

3. E-Safety issues, Head of E-safety- Timothy Smith - t.smith@cga.school

4. Online bullying, the Dean of School SH – Mr. Kenneth Knight – k.knight@cga.school.nz
   the Dean of School NH - Mr. Andrew Daniel - a.daniel@cga.school.nz

Appendix 1 - Details taken from the CGA rules and regulations document:

Cyberbullying

Cyberbullying is an unpleasant and insidious form of bullying which uses information and communication technology to support deliberate, repeated and hostile behaviour by an individual or group that is intended to emotionally harm others.

CGA recognises the following situations may be interpreted as cyberbullying and will take the necessary actions to sanction those involved.

Bullying via online communications by various electronic media may include but are not solely restricted to:

a. texts, instant messages on the Zoom app or other communication programmes
b. the use of camera images, taken from Zoom lessons to cause distress, fear or humiliation.
c. the use of mobile phone camera images taken of the online lessons or when the students physically meet up to cause distress, fear or humiliation.
d. Posting threatening, abusive, offensive or humiliating material or comments on websites (including blogs, personal websites and social networking sites such as Facebook, Instagram, Twitter, YouTube, Snapchat)
e. Using dating apps, (such as Tinder or Grinder) to cause upset or abuse.
f. Using email to message others in a threatening or abusive manner
g. hijacking/cloning email accounts.

Behaviour whilst in online classroom or in onsite lessons, field trips.

For most of the CGA students the online classroom format will be new and exciting. With this in mind, the teacher will use his or her own discretion as to what they deem courteous.

a. Students are expected to behave in a courteous manner at all times whilst involved in an online or onsite lesson.
b. Students should not be eating during an online lesson; except for health reasons
c. During lessons students should not be **privately** messaging each other via Facebook, Instagram, SnapChat or any other communication software.
d. During lessons students should not talk over their peers or the teacher.

E-Safety

It is the duty of CGA to ensure that every student in its care is safe in the digital world.

Using the CGA technology to learn.

All students are issued with their own personal school email addresses and usernames for use on our network. This includes; Managebac, Zoom and Slack and Gmail.

a. Access to all of the online platforms used at CGA is via a personal login, which will be password protected.

    1. Students are regularly reminded of the need for password security. use a strong, unique password consisting of at least 16 characters. This should include a mixture of capital and lowercase letters, numerals and special characters. It must not include a group of three characters from the username.
    2. As a matter of good practice it should be changed every 6 months.
    3. never share their passwords.

b. LMC may be regarded as safe and secure and must be used when submitting homework.

c. Students should be aware that communications through Slack, LMC, Zoom and school email addresses can and will be monitored.

d. Students must only use their school accounts to email staff; they must not seek to contact staff via private email or social media accounts.

e. Students must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature, and should immediately report such a communication to the Dean/counsellor.

f. The School expects students to think carefully before they post any information online, or re-post or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

g. Students must report any accidental access to materials of a violent or sexual nature directly to their Dean/Counsellor.

h. The deliberate accessing of inappropriate material by a student will lead to the incident being recorded on their file and will be dealt with under CGA's Behaviour, Rewards and Sanctions Policy.

Use of digital and video images

Digital imaging technologies have created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet.

Students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying, stalking or grooming. Also, digital images may remain available on the internet indefinitely thus causing harm or embarrassment to individuals in the short or longer term.

With this in mind:

a. Students must not take, use, share, publish or distribute images of others or themselves, except when in connection with a clear educational purpose and/or authorised to do so by staff and the students themselves.

b. CGA will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police. If the School discovers that a child or young person is at risk as a consequence of online activity (this is covered in greater detail in the child protection policy), it will seek assistance from the Police immediately.

c. Incidents of misuse or suspected misuse will be dealt with by staff in accordance with the School's policies and procedures.

Appendix 2 – Acceptable use of technology policy

Scope of this Policy

This policy applies to all members of the School community who have access to the School's IT systems, including staff, students and parents. In this policy 'staff' includes teaching and non-teaching staff, governors and regular volunteers. 'Parents' includes student's carers.

The policy applies to all use of the School's computer systems, including access to those systems using personal devices, and all use of computers (including personal devices) in connection with school activities.

Online behaviour

1. As a member of the school community, you should follow these principles in **all** of your online activities.

2. Ensure that your online communications, and any content you share online, are respectful of others.

3. Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene or promotes violence, discrimination or extremism).

4. Respect the privacy of others. Do not share photos, videos, contact details or other information about members of the school community without their permission, even if the content is not shared publicly.

5. Do not access or share material that infringes copyright, and do not claim the work of others as your own.

6. Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities. Any illegal activity may be reported to the police.

7. Staff must not communicate with students using personal email or social media accounts. Likewise, students must not communicate with staff using personal email or social media accounts.

Using the School's IT systems

Whenever you use the School's IT systems, you should follow these principles:

1. Only access school IT systems using your own username and password.

2. Do not share your username or password with anyone else inside or outside of CGA.

3. Do not attempt to circumvent the content filters or other security measures installed on the School's IT systems.

4. Do not attempt to access parts of the system which you do not have permission to access or look for vulnerabilities in the systems.

5. Do not attempt to install or run your own software on, or otherwise alter, school IT systems.

6. Do not vandalise the School's IT systems. Vandalism includes destroying files created by others, and any action which disrupts the normal operation of the systems.

7. You should take care regarding the contents and validity of all emails you receive.

8. You must never open hyperlinks in emails or any attachments to emails unless you know and trust the sender and are confident that the email is genuine.

9. Remember that the IT systems are there to enable educational, school-related activities.

10. Remember that the School monitors use of its systems and can view content accessed or sent via its systems.

Compliance with related school policies

You must ensure that you comply with the School's E-Safety Policy, along with all other school policies.

Breaches of this policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the School's usual procedures. Serious misconduct could lead to permanent exclusion or dismissal.

In addition, a deliberate breach may result in the School restricting your access to school IT systems.

If you become aware of a breach of this policy or the E-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online, you should report it to the Designated Safeguarding Lead or E-Safety Coordinator.