INTERNAL PROCEDURE

Title: Online Safety for Students

POLICY HOLDER:	**Assistant Principal Student Services**
SMT OWNER:	**Vice Principal Student & College Services**
VERSION NO:	**5**
LAST REVIEWED:	**April 2024**

This document is meant for electronic viewing and is maintained as part of the college document control procedure. It is uncontrolled if viewed in hardcopy, printed format.

Accessibility: If you would like this information in an alternative format, e.g. Easy to Read, large print, Braille or audio tape, or if you would like the procedure explained to you in your language, please contact the College's marketing team on 01603 773 169.

Further information: If you have any queries about this policy or procedure, please contact the named policy holder.

EASTON COLLEGE

PASTON COLLEGE

CITY COLLEGE NORWICH

City College Norwich, Ipswich Rd, Norwich NR2 2LJ

Amendments log

Review date	Version	Changes	Originated by	Approval
04.01.17	2		Alex Wallace	SMT
17.07.18	3	Annual update Inclusion of GDPR	Cat Warrington, HRH	SMT
15.07.19	4	Annual update	Marie Pacey HRH	SMT
02.04.24	5	Annual update throughout including appendices and specific changes made to: 1.6: Inclusion of 4 key areas of risk: content contact conduct and commerce 6.3: Legal requirements including internal procedures 7: complete overhaul and update to Roles and Responsibilities section to include Governors and the Principal and DSL and links with Executive Director IT Services responsibilities. 11: overhaul and of section and description of what students will learn	HRH	SMT

Contents

1. Procedure statement

1.1 City College recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all students and staff and encourage the use of technologies to enhance skills, promote achievement and enable lifelong learning.

1.2 However, the accessibility and global nature of the online world and different technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the college whilst supporting students to identify and manage risks independently and with confidence.

1.3 We believe this can be achieved through a combination of security measures, teaching, guidance and implementation of our policies. In furtherance of our duty to safeguard, we will do all that we can to make our students and staff stay safe by recognising unsafe situations and understanding what to do if something goes wrong.

We aim to have clear mechanisms to identify, intervene and escalate an incident, where appropriate

1.4 This online safety procedure should be read alongside other relevant college policies e.g. Safeguarding, Student IT Acceptable Usage Policy, Anti Bullying and Harassment and Student Disciplinary.

1.5 This procedure includes the College's **Social Media Guidelines** in Appendix 3

1.6 The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Creation, Monitoring and Review

2.1 This procedure was originally developed with our online safety group. The group was made up of different stakeholders including a Safeguarding Officer, a senior line manager, a member of the IT support team, students, members of teaching staff, members of support staff and parents as well as our local community police support officer.

2.2 Consultation regarding the content of this procedure has been carried out where it is appropriate and timely to do so. This has been through staff CDP sessions (Code of Conduct, Child Criminal Exploitation and Safeguarding training) and meetings with a selection of staff, stakeholders and students.

2.3 The impact of the procedure will be monitored regularly with a full review being carried out at least once a year. The procedure will also be reconsidered where particular concerns are raised or where an online safety incident has been recorded.

3. Procedure Aims and Objectives

3.1 The aims of this Procedure are to;

- provide a clear outline for students demonstrating how we will support them to use social media and new technologies in a safe way so that it enhances their learning and enjoyment whilst safeguarding their wellbeing.
- define clearly our expectations of student behaviour in relation to online safety and the college's approach when breaches or infringements occur.
- outline what is acceptable and not unacceptable use of college technologies.

3.2 The purpose of this procedure and guidelines is:

- to encourage good practice
- to protect the College and its students
- to clarify where and how existing policies and guidelines apply to social media and online safety
- to promote effective and innovative use of social media as part of the College's activities

4. Definitions

4.1 This procedure defines online safety, as the safe use of

- Your online persona
- Your use of social media sites both internal and external to the College
- Your use of mobile technologies such as texting and sexting
- Your online behaviour and interaction with others
- Your personal data and security
- An online safety incident is defined as putting yourself or someone else at risk online.

4.2 The term social media is used to describe dynamic and socially-interactive, networked information and communication technologies by which personal information or opinions can be presented for public consumption on the Internet. Examples include: Apps with Social functioning e.g. snapchat or games with social features etc, blogs and vlogs, websites, messaging apps, messaging services and social networking sites.

5. Scope

5.1 This procedure applies to all students who have access to the college IT systems, both on the premises and remotely.

5.2 The online safety procedure applies to all use of the internet and forms of electronic communication including but not limited to email, mobile phones and social media sites.

5.3 Any user of college IT systems must adhere to the IT Acceptable Use Policy (available on the Help tile on the Home Page.) this includes using free Wi-Fi, which is monitored by the College.

6. Legal requirements

6.1 The Education Act[1] requires further education colleges to make arrangements to ensure that their functions are carried out with a view to safeguarding and promoting the welfare of children.

6.2 Everyone who comes into contact with children and their families has a role to play in safeguarding children. College staff are particularly important as they are in a position to identify concerns early and provide help for children, to prevent concerns from escalating. Institutions and their staff form part of the wider safeguarding system for children. This system is described in statutory guidance *Working Together to Safeguard Children*. [2] Institutions should work with social care, the police, health services and other services to promote the welfare of children and protect them from harm.

6.3 This procedure has been checked against the current guidance applicable to institutions which is:

- Keeping Children Safe in Education
- Working Together to Safeguard Children
- Sharing nudes and semi-nudes: advice for education settings, UKCCIS
- The Prevent Duty and protecting children from radicalisation
- Filtering and monitoring standards for schools and colleges

It also refers to internal procedures or documents

- Searching students procedure
- Anti bullying and harassment
- Student Disciplinary
- Student IT Acceptable Usage Policy
- Safeguarding Code of Conduct for Staff

6.4 Artificial intelligence (AI)

[1] https://www.legislation.gov.uk/ukpga/2002/32/section/175 accessed 02/04/24

[2] https://assets.publishing.service.gov.uk/media/65cb4349a7ded0000c79e4e1/Working_together_to_safeguard_children_2023_-_statutory_guidance.pdf accessed 02/04/24

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

The key principle in our approach is that students should be protected from harm through education and raising awareness of the associated risks of AI technology, also through effective filtering and monitoring and self-reporting to staff where they are worried.

The college recognises that AI has many uses to help students learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. Other risks may emerge with time and there are other college policies which will help to manage these (plagiarism, online safety, IT acceptable use.)

The College will treat any use of AI to bully students in line with our anti-bullying and harassment procedure.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the college.

7 Roles and Responsibilities

7.1 There are clear lines of responsibility for online safety within the College. The first point of contact where there is an identified risk of harm to the student or someone else, should be the Safeguarding Officer.

7.2 All staff are responsible for ensuring the safety of students and should report any online safety concerns **where the student's wellbeing is at risk** immediately to the Safeguarding Officer using the procedure outlined in the college's Safeguarding procedure.

7.3 **Other incidents which are not related to an immediate risk of harm,** will be dealt with using the appropriate college procedure including but not limited to Anti-Bullying and Harassment, Student Disciplinary and the Student Acceptable Use procedures. See Figure 1 below:

Is the student at immediate risk of harm?	Yes	Safeguarding referral	**What to do if you are worried about a student** If you are concerned about the safety of a student you must refer this to the Safeguarding team. You do this by making a referral through the red Report Safeguarding button on our homepage or via the student's ILP. For urgent disclosures that require immediate attention call the safeguarding mobile phone number. **Safeguarding mobile phone numbers:** • Marie Pacey 07795 487645 • Charlotte Hardiment 07717 484142 • Sam Warner 07772 785346 **Designated Safeguarding Leads are:**
You are informed about the exchange of sexualised images of a student U18	Yes	Safeguarding referral	
There is a risk of a student making a decision(s) online, with no understanding of how to keep themselves safe or make the situation safer. Examples could include uninformed financial choices or investments or a risk of financial abuse or blackmail.	Yes	Safeguarding referral	

			• Jerry White • Helen Richardson-Hulme • Jacky Sturman • Jo Kershaw • Sebastian Gasse • Mat Scott • John Pollitt		
Allegation of bullying or harassment online.	Yes	Follow the Bullying and Harassment procedure	Course Lead and Head of Area responsibility		
There is a wellbeing need for the student in dealing with online issues and friendships	Yes	Refer to the Wellbeing team	wellbeing@ccn.ac.uk		
Student is misusing College IT systems or other allegation of misconduct	Yes	Student Disciplinary procedure	Course Lead or Head of Area to oversee the process		

7.4 All teaching staff are required to deliver online safety awareness as part of student induction and to read through and adhere to the incident reporting procedure. Helpful resources for this are provided on SharePoint on the Personal Development tab.

7.5 When informed about an online safety incident, staff members cannot guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

7.6 All students must know what to do if they have online safety concerns and who to talk to. In most cases, this will be their teacher or the college's Safeguarding Officer.

Governors

The governing board has overall responsibility for monitoring this policy and holding the Principal and DSLs to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure students are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the College has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the college in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the college.

Designated Safeguarding Lead

Details of the college's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Principal in ensuring that staff understand this procedure and that it is being implemented consistently throughout the school
- Working with the Principal and governors to review this procedure annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Executive Director IT Services to make sure the appropriate systems and processes are in place
- Working with the Principal, DSLs and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the college's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this procedure

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the college's student anti bullying and harassment procedure
- Updating and delivering staff training on online safety alongside safeguarding training
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in college to the Principal and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

The Executive Director IT Services is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at college, including terrorist and extremist material
- Ensuring that the college's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the college's ICT systems on a [weekly/fortnightly/monthly] basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this procedure
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the college procedure

This list is not intended to be exhaustive.

Safeguarding Officer

7.7 The Safeguarding Officer is responsible for keeping up to date with new technologies and their use, as well as attending relevant training. Parents and carers can access regular Safeguarding updates that are sent to staff via the Safeguarding page on the website.

Staff responsibilities

7.8 All staff are responsible for using college IT systems and mobile devices in accordance with the college Safeguarding, Code of Conduct and Conditions of Use policies. Staff are responsible for attending staff training on online safety and always displaying a model example to students through embedded good practice.

7.9 All digital communications with students must be always professional and be carried out in line with the college Code of Conduct. Online communication with students using the college network or external platforms not hosted by the college, such as social media sites, may be used in line with the college Code of Conduct.

Student responsibilities

7.10 Students are responsible for using the college IT systems and mobile devices in accordance with the college Student IT Acceptable Usage Policy, Social Media Guidelines and online safety Rules.

7.11 Students must act safely and responsibly at all times when using the internet and/or mobile technologies. They are responsible for attending online safety lessons as part of their induction and are expected to know and act in line with other relevant college rules e.g. mobile phone use, sharing images, cyber-bullying etc.

7.12 Students must tell a member of staff they trust where they are worried or concerned, or where they believe an online safety incident has taken place involving them or another member of the college community.

7.13 Students must remember to check their college email, this is where they will receive important course and college information. All College communications go to students' College email and not personal email addresses. It will be assumed that students have read all emails sent by the college within 5 working days of the email being sent. Staff[3] will help students to set up their college email account on their phone if requested.

8 Student behaviour

8.1 The college will not tolerate any abuse of IT systems. Whether offline or online, communications by students should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student disciplinary procedure.

8.2 Where conduct is found to be unacceptable, the college will deal with the matter internally and may remove access permissions in individual cases. Where conduct is considered illegal, the college will report the matter to the police.

8.3 Students must never share their passwords or leave their computer logged on (for example when going to use the printer.)

8.4 All students using mobile devices are expected to behave in a responsible manner respecting the rights and needs of other users. Personal entertainment systems should be used in a manner that does not disturb other users and general noise should be kept to a minimum, especially in open access environments.

9 Security

9.1 The college will do all that it can to make sure the college network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of college systems

[3] Staff in IT Services or the Student's Union

and information. Digital communications, including email and internet postings, over the college network, will be monitored in line with the college Conditions of Use procedure.

10 Use of Images and Video

10.1 All students should consider the risks when taking, downloading and posting images online and making them available to others. There are particular risks where personal images of themselves or others are posted onto social networking sites, for example.

11 Education and Training

11.1 With the current unlimited nature of internet access, it is impossible for the college to eliminate all risks for staff and students. It is our view therefore, that the college should support staff and students stay e-safe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

For students:

11.2 Students will attend online safety lessons as part of their induction to the college. Issues associated with online safety online safety apply across the curriculum and students should receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies. Students should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search.

11.3 Within classes, students will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

11.4 By the end of College, younger students age 16-18 will have been taught:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

Adult students and Apprentices will be supported with much of the learning listed above through naturally occurring opportunities within the classroom, induction, through individual conversations with staff including safeguarding and wellbeing team where appropriate. Adult students and Apprentices may also engage with online safety through enrichment guest speaker visits such as from the Police Cyber Choices Team.

12 Procedure- Incidents and Response

12.1 Where an online safety incident is reported to the college this matter will be dealt with very seriously. If the incident places a student at risk or compromises their wellbeing this will be reported through the Safeguarding procedure.

12.2 Other incidents will be dealt with using the appropriate college procedure including but not limited to Anti-Bullying and Harassment, Student Disciplinary and Conditions of Use procedures.

12.3 The college will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a student wishes to report an incident, they can do so to their teacher or to the college Safeguarding Officer.

12.4 Where a member of staff wishes to report an incident where a student's wellbeing is at risk, they must follow the safeguarding procedure. Following any incident, the college will review what has happened and decide on the most appropriate and proportionate course of action.

12.5 Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. This is in line with the college Conditions of Use Procedure.

12.6 Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies, including contacting the police.

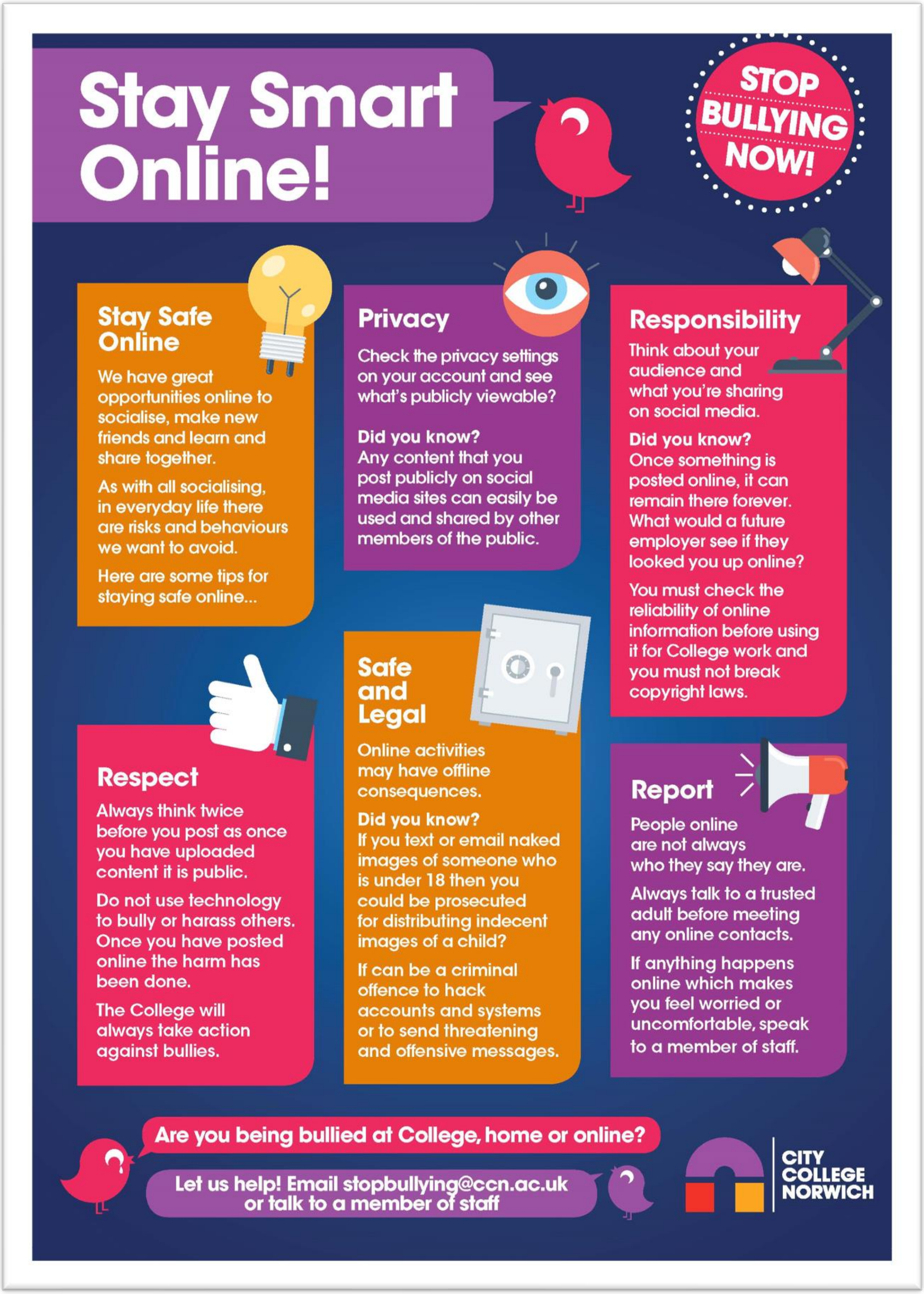
13 References to related College policies

- Safeguarding procedure
- Code of Conduct for Staff
- Student IT Acceptable Usage Policy
- Anti-Bullying and Harassment procedure

14 Feedback and Contact

14.1 The College welcomes all constructive feedback on this and any other college procedure. If you would like further information on online safety or wish to send us your comments on our online safety Procedure, then please contact the Procedure Holder at the front of this document.

Appendix 1 – Online safety awareness



Stay Smart Online!

STOP BULLYING NOW!

Stay Safe Online

We have great opportunities online to socialise, make new friends and learn and share together.

As with all socialising, in everyday life there are risks and behaviours we want to avoid.

Here are some tips for staying safe online...

Privacy

Check the privacy settings on your account and see what's publicly viewable?

Did you know?
Any content that you post publicly on social media sites can easily be used and shared by other members of the public.

Responsibility

Think about your audience and what you're sharing on social media.

Did you know?
Once something is posted online, it can remain there forever. What would a future employer see if they looked you up online?

You must check the reliability of online information before using it for College work and you must not break copyright laws.

Respect

Always think twice before you post as once you have uploaded content it is public.

Do not use technology to bully or harass others. Once you have posted online the harm has been done.

The College will always take action against bullies.

Safe and Legal

Online activities may have offline consequences.

Did you know?
If you text or email naked images of someone who is under 18 then you could be prosecuted for distributing indecent images of a child?

It can be a criminal offence to hack accounts and systems or to send threatening and offensive messages.

Report

People online are not always who they say they are.

Always talk to a trusted adult before meeting any online contacts.

If anything happens online which makes you feel worried or uncomfortable, speak to a member of staff.

Are you being bullied at College, home or online?

Let us help! Email stopbullying@ccn.ac.uk or talk to a member of staff

CITY COLLEGE NORWICH

Social Media Guidelines

Use of Social Media: Best Practice Guidelines for Students

1. Student responsibilities

- You must not use your site to attack or abuse staff, students or others.

- You should respect the privacy and the feelings of others.

- You must not include contact details or pictures etc. of other students, members of staff without their prior permission.

- Remember that if you break the law on your site (for example by posting something defamatory), you will be personally responsible.

- You should not use your site or pages in any way that may compromise your current or future employability.

- Any content that you post about yourself or others could be brought to the attention of the College, future employers or professional bodies and may be detrimental to your studies and/or future career.

- Students need to exercise caution when considering social interaction with staff, or employers from a placement setting. Students should only contact staff and work placement employers through their College email.

- Where Social Media is utilised as part of a research study or project; all ethical considerations and requirements of the College and course of study should be adhered to.

- Don't reveal confidential information about the College or its staff, students, partner organisations. This might include aspects of College procedure or details of either internal or private discussions.

- College groups may use the college logo but in accordance with the brand guidelines. Contact New Media department for advice.

- If someone from the media or press contacts you about posts on your site which relate to the College you should discuss it with the New Media department.

- You must avoid bringing the College into disrepute in any way.

- If you already have a personal social networking site or intend to initiate; you should not declare, imply or indicate that your content or views are representative of the College.

- If in any doubt, you may want to discuss your site content with the Marketing department. You may also want to include a simple and visible disclaimer such as "these are my personal views and not those of the College".

Contacts

Richard Steer
Senior Communications and PR Officer
richard.steer@ccn.ac.uk

Emily Smart
Senior Marketing and Events Officer
emily.smart@ccn.ac.uk

Sophie Watson
Interim Marketing Manager
sophie.watson@ccn.ac.uk

IT Services
John Pollitt Executive Director IT and Designated Safeguarding Lead
john.pollitt@ccn.ac.uk

Safeguarding Officer mobile phone numbers:
Marie Pacey 07795 487645
Charlotte Hardiment 07717 484142
Sam Warner 07772 785346 direct dial 01603 732326.

Designated Safeguarding Leads are:
Jerry White
Helen Richardson-Hulme
Jacky Sturman
Jo Kershaw
Sebastian Gasse
Mat Scott
John Pollitt

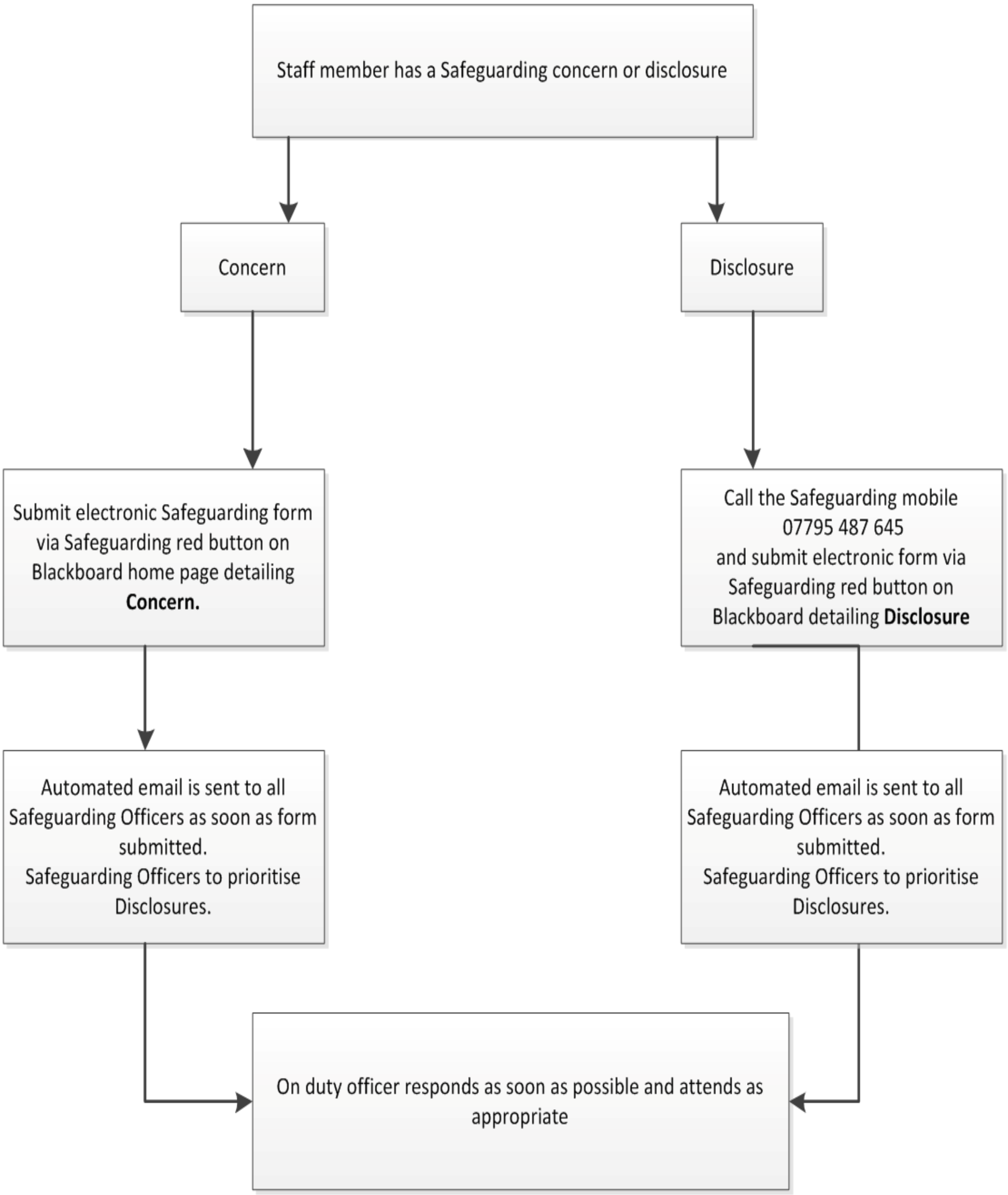
Reporting online safety incidents

Guidance for dealing with an online safety incident

All staff are responsible for ensuring the safety of students and should report any online safety concerns **where the student's wellbeing is at risk** immediately to the Safeguarding Officer using the procedure outlined in the college's Safeguarding procedure.

Other incidents will be dealt with using the appropriate college procedure including but not limited to Anti-Bullying and Harassment, Student Disciplinary and Conditions of Use procedures.

Safeguarding procedure


Staff member has a Safeguarding concern or disclosure
Concern
Disclosure
Submit electronic Safeguarding form via Safeguarding red button on Blackboard home page detailing **Concern.**
Call the Safeguarding mobile 07795 487 645 and submit electronic form via Safeguarding red button on Blackboard detailing **Disclosure**
Automated email is sent to all Safeguarding Officers as soon as form submitted. Safeguarding Officers to prioritise Disclosures.
Automated email is sent to all Safeguarding Officers as soon as form submitted. Safeguarding Officers to prioritise Disclosures.
On duty officer responds as soon as possible and attends as appropriate

Student IT Acceptable Usage Policy

Acceptable usage

There are key themes outlined in this procedure for students. They are

1. Use of IT on all sites is closely monitored
2. Keep your IT account secure with a strong password & lock your PC if you need to step away from it
3. Always store your data on the network or within Office 365 (avoid USB drives)
4. Don’t access or display offensive material
5. Regularly scan your devices for viruses or malware
6. Don’t disconnect or move IT equipment
7. Stay within the law and stay safe

Key messages:

Never let anyone know your password or let anyone else log on using your account. You are responsible for the security of your account and the files stored therein.

Users will be held responsible for any misuse attributed to their account; this could include misuse by other people.

The College does not tolerate harassment in any form whatsoever.

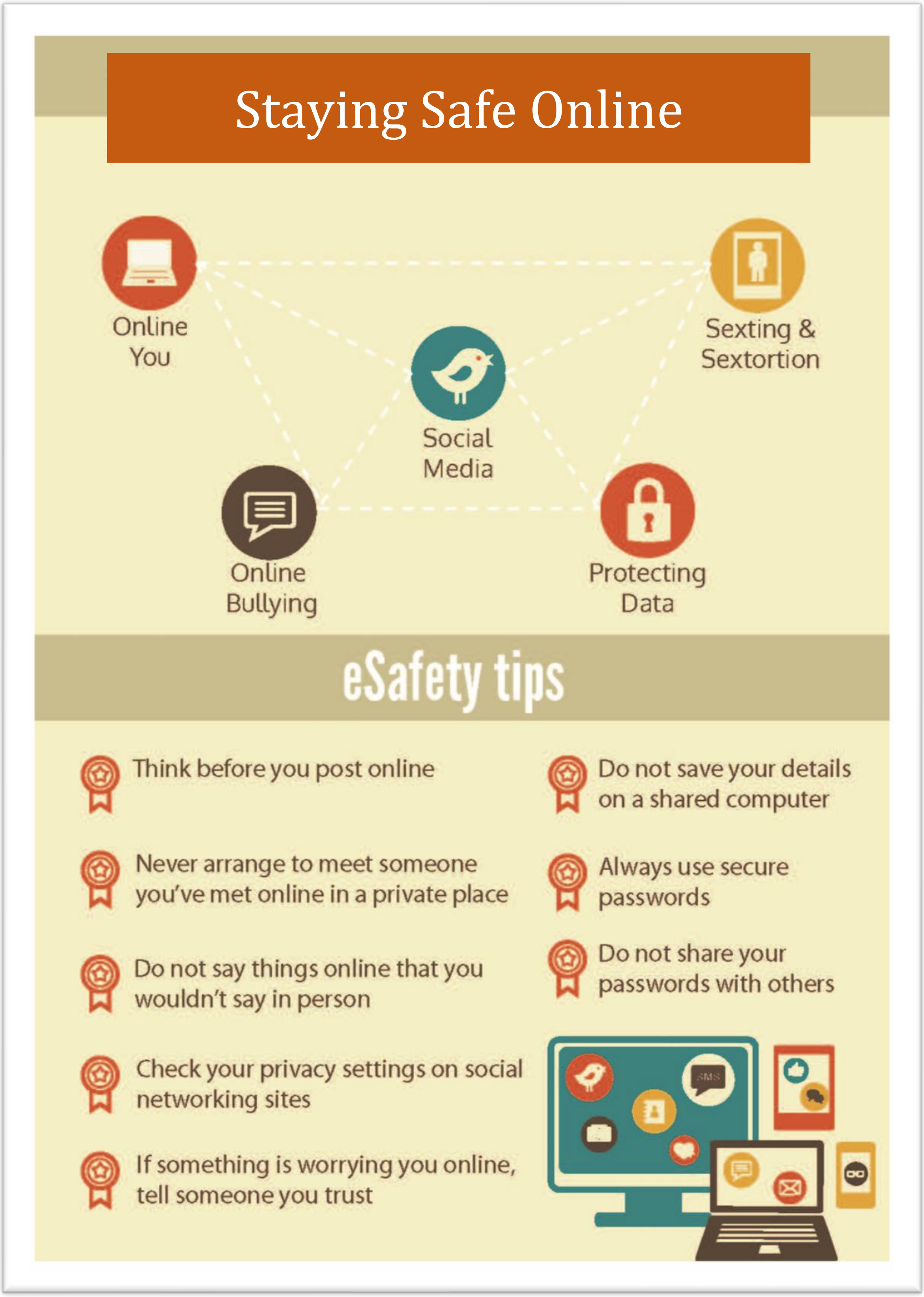
You must not store, print, display, or transmit

- Obscene, pornographic, discriminatory, defamatory or other material that may offend
- Material that infringes a right or inherent right of another person
- Material that is designed or likely to cause annoyance, inconvenience or needless anxiety
- Material that is designed to be extremist or to radicalise

Mail or other communications should not be sent to those who do not, or may not, wish to receive it. Use of email to send unsolicited email (SPAM) to other users may result in the loss of your email account.

Offensive material should never be transmitted through the email system.

Online safety tips



Staying Safe Online

Online You

Sexting & Sextortion

Social Media

Online Bullying

Protecting Data

eSafety tips

- Think before you post online
- Never arrange to meet someone you've met online in a private place
- Do not say things online that you wouldn't say in person
- Check your privacy settings on social networking sites
- If something is worrying you online, tell someone you trust
- Do not save your details on a shared computer
- Always use secure passwords
- Do not share your passwords with others

UK GDPR/Data Protection Act 2018:

UK GDPR/Data Protection Act 2018 helps to protect your privacy and any personal data related to you.

When organisations ask you for personal details (e.g. your name, date of birth, address, a picture of you etc) they must say how they are going to use the information, and only use the data for this purpose.

They must not hold the information for any longer than necessary for this purpose.

You have the right to ask for a copy of this information (a "Subject Access Request"), and in certain circumstances to ask for it to be deleted (right to erasure).

You should be aware that different countries have different privacy laws; in particular, laws in countries outside the European Union, including the USA, can be very different to ours. This is particularly important when using online systems such as social media as it's not always obvious in which country these systems are based.

For more information on how the College manage your data please see the Student Privacy Notice available via the College website.

For more information about Data Protection please see Information Commissioner's Office website, and in particular https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

For help in College contact the Information Compliance Officer:

Information Compliance Officer
Tel +44 (0)1603 773585

Email: data_protection@ccn.ac.uk
http://www.ccn.ac.uk