# ICT Administration and E-SAFETY POLICY

## Contents

## ICT ADMINISTRATION AND E-SAFETY

### Rationale

This policy is designed to promote an ICT culture providing equal and open, yet safe, access to ICT facilities which empowers pupils, teachers and administrators to make the fullest and most appropriate use of ICT in their day to day work and leisure.

### Linked policies and cross-references

- Safeguarding Policy;
- Health and Safety Policy;
- KCSIE (2018),
- GDPR Privacy Notice March 2018

### E-Safety risks for those who have access to the College ICT system

The use of exciting and innovative ICT tools in educational institutions and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the College. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, the loss of or the sharing of personal information
- The risk of grooming by those with whom they make contact on the internet.
- The sharing or distribution of personal images without an individual's consent or knowledge
- Inappropriate communication or contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video or internet games
- An inability to evaluate the quality, accuracy, appropriateness and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and on the learning of the young person.
- Radicalisation through internet sources

Many of these risks reflect situations in the off-line world and it is essential that this e-Safety policy is used in conjunction with other College policies (e.g. no bullying and safe-guarding policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to online risks and minimise exposure, so that they have the confidence and skills to face and deal with these risks.

**Monitoring**

The College will monitor the impact of the policy using:
- Logs of reported incidents
- Internal monitoring data for network activity

**Scope of the Policy**

This policy applies to all members of the College community (including staff, pupils, parents and visitors). In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers (but access to systems is not intended in any way to imply an employment relationship). 'Parents' include, where applicable, pupils' carers and those with parental responsibility. 'Visitors' includes anyone else who comes to the College, including occasional volunteers. The Education and Inspections Act 2006 empowers Principals, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the College site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-Safety incidents covered by this policy, which may take place out of College, but is linked to membership of the College.

**Roles and Responsibilities**

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

*Principal:*

- 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 Designated Safeguarding Lead.
- The Principal is responsible for ensuring the relevant staff receive suitable CPD to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.
- The Principal is 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 Coordinator (Designated Safeguarding Lead):*

- Takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the College E-Safety policies and documents.
- Meets regularly with the Principal and Director of ICT to discuss current issues, review incident logs.
- Reports to the SMT when necessary and ICT committee.
- Ensures that they keep themselves 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.

- Ensures that the use of the network including remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Coordinator or Principal
- 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.
- Receives reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments.

*The Designated Safeguarding Lead*

should be trained in e-Safety issues and be aware of the potential for serious child protection issues which may arise from:

- Sharing of personal data.
- Access to illegal or inappropriate materials.
- Inappropriate on-line contact with adults or strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

*Director of ICT*

- Ensures that the College meets the e-Safety technical requirements
- Ensures that users may only access the College' networks through a properly enforced password protection policy.
- Ensures that monitoring software and systems are implemented and updated as agreed in College policies.
- Assists the E-Safety Coordinator with reviewing and monitoring the College e-Safety policy and documents.

*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 ICT Acceptable Use Policy and Staff Code of Conduct.
- They report any suspected misuse or problem to the e-Safety Co-ordinator
- Digital communications with pupils are on a professional level only.
- E-Safety issues are embedded in all aspects of the curriculum and other College activities.
- Pupils understand and follow the College e-Safety and Student acceptable use policies.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extra-curricular and extended College activities. They are aware of e-Safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current College policies with regard to these devices.

*Pupils:*

- Are responsible for using the College ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to College systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand College guidance on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand College policies on the taking and use of images and on cyber-bullying.
- Should understand the importance of adopting good e-Safety practice when using digital technologies out of College and realise that the College's e-Safety Policy covers their actions out of College, if related to their membership of the College.

*Parents/Guardians:*

Parents and Guardians play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The College will therefore take the opportunity to help parents understand these issues through parents' evenings, letters, and other literature. Parents and guardians will be responsible for endorsing (by signature) the Pupil Acceptable Use Policy.

Staff and parents may get further advice from the following websites

CEOP – https://www.ceop.police.uk/safety-centre/
Net-Aware - https://www.net-aware.org.uk/
Thinkuknow - https://www.thinkuknow.co.uk

## E-Safety Education

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

- An e-Safety induction is provided at the beginning of each academic year for all new staff and all new students entering the College. This will cover both the use of ICT and new technologies in College and the dangers outside College.
- This is reinforced in PSHE, ICT and other classes.
- Key e-Safety messages will be reinforced as part of a planned programme of training by the e-safety officer.
- Pupils are taught in PSHE lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils are helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside College.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet in PSHE and other classes.

**E-Safety and Prevent Duty**

Whilst pupils are not permitted to access social networking sites in College time, pupils are educated in best practice through seminars, the PSHE and general teaching curriculum and via tutors as part of the College's pastoral care system:

CIC encourages children to talk openly with their parents or guardian about what they see online and should always tell them if anyone asks for personal information.

Students must commit to follow the family and College rules about safety on the Internet and when playing online games.

It is essential that students understand and commit to not sharing personal information with anyone they meet online. This includes their real name, address, phone number, financial information, College name, passwords, or other private information.

Although many students in the sixth form know basic ways to stay safe while online, they must also commit to ethical online users.
Such as:

- Post only what you would feel comfortable with the whole world seeing, including parents or College personnel.
- Never use the Internet to spread gossip, bully or hurt someone's reputation. Students should understand what security tools are available to use on most computers to further protect themselves, their personal information, and their computer from viruses, spyware, and spam.
- Students must also understand that they are in charge of their online experience and should manage it the way they would in the real world.
- Students are taught to be aware of potentially untrustworthy influences online as part of our Prevent duty. People who try to influence them online about their beliefs and ideas should not be trusted.
- If something or someone online makes pupils feel uncomfortable, they have the right to not respond, delete a post, and most importantly tell a trusted adult.
- Students must commit to never meet in person with someone they met online.

**Staff**

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

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:

- Formal e-Safety training will be made available to staff via the *Educare* online teaching module, either at inset or as soon as a new member of staff joins the College.
- All new staff should receive e-Safety training as part of their induction programme, ensuring that they fully understand the College e-Safety policy and Acceptable Use Policies.

- The e-Safety co-ordinator receives regular updates through attendance at training sessions and by reviewing any guidance documents released.
- This e-Safety policy and its updates will be presented to and discussed by staff in staff INSET days.
- The e-Safety coordinator will provide advice, guidance and training to individuals as required.

**Technical Infrastructure**

The College will be responsible for ensuring that the College infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- There will be regular reviews and audits of the safety and security of College ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to College ICT systems.
- All users will be provided with a username and password by the ICT department who will keep an up to date record of users and their usernames. Users will be advised to change their password regularly.
- The “master administrator” passwords for the College ICT system, used by the Network Manager must also be available to the Principal or HR Manager.
- 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 a managed filtering service.
- 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.
- Users should report any actual or potential e-Safety incident to the e-Safety Officer.
- An agreed procedure is in place for the provision of temporary access of “guests” (e.g. trainee teachers, visitors) onto the College system where they are given their own log on and restricted access.
- The College infrastructure and individual workstations are protected by up to date virus software.
- Personal data should not 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 pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where pupils 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 can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

**Use of Digital and Video Images**

- When using digital images, staff should inform and educate pupils 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 or video images to support educational aims, but must follow College policies concerning the sharing, distribution and publication of those images.
- Care should be taken when taking digital or video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the College into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Photographs of pupils used in the College magazines, other College publications, the College website and other promotional literature will only be used in accordance with the Parent College Contract.

**Data Protection**

The Head of Computing is the nominated ‘Data Champion’ at Chelsea Independent College who works on behalf of the Data Controller (Astrum Education) to deal with all your requests and enquiries concerning the College’s uses of your personal data and endeavour to ensure that all personal data is processed in compliance Data Protection Law. Please refer to the College’s Privacy Notice for further information about how the College will use (or ‘process’) personal data about individuals.

**Communications**

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

- The official College email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored.

- Users must immediately report, to a suitable person – the receipt of any email that makes them feel uncomfortable, is offensive or threatening in nature and must not respond to any such email.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the College website and only official email addresses should be used to identify members of staff.

**Responding to Incidents of Misuse**

Listed below are the responses that may be made to any apparent or actual incidents of misuse. Where more than one possible sanction is listed the response will be determined by the nature and severity of the incident.
If any apparent or actual misuse appears to involve illegal activity i.e.

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

the Principal should be informed immediately and all actions taken to preserve the evidence.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the College community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through behaviour and disciplinary procedures.

**Filtering**

*Students*

The College will maintain a "best effort" filtering policy to restrict students' access to inappropriate sections of the internet. The College expects all users to use the internet responsibly and will make a "best effort" to prevent students visiting internet sites that contain or relate to:-

- Pornography (including child pornography)
- Promoting discrimination of any kind
- Promoting racial or religious hatred Promoting illegal acts
- Any information that may be offensive to other pupils or staff.

Students' access will be monitored and any apparently inappropriate sites will be blocked. The use of proxy sites to by-pass the College filter will also be monitored and these will also be blocked.

*Staff*

Staff are allowed unfiltered access to the internet, but their use is logged and archived.
If necessary this can be audited, but only at the request of the Principal/Executive Principal.

Staff may request blocked sites to be made available to students if they contain information relevant to their subjects. These sites should be blocked again when no longer required for research. Requests should be made to the Director of ICT

### Further Information and Training

- **What pupils and parents can do:** Pupils are encouraged to talk to their family members and friends about how they can stay safe online, whether they are using social media, shopping online or connecting with the latest wearable.
- **Materials to help you do it:** StaySafeOnline.org offers tips and advice about raising good digital citizens – what to watch for and how to get the conversation started.
- **Staff training** is offered through the online training software: Educare. All staff who come into regular contact with children will be asked to complete the online training in Online Safety.

### Breach reporting

The law requires the College to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the College regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the College's systems, e.g. through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The College must generally report personal data breaches to the ICO without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the College must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or pupils become aware of a suspected breach they should notify the College Data Champion (Head of Computing) with immediate effect.

Data breaches will happen to all organisations, but the College must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The College's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

**Breaches of this policy**

A deliberate breach of this policy will be dealt with as a disciplinary matter using the College's usual procedures. In addition, a deliberate breach may result in the College restricting your access to College IT systems.

If you become aware of a breach of data you should report your concerns to the Data Champion (Head of Computing), or you are concerned that a member of the College community is being harassed or harmed online you should report e-safety concerns to the Designated Safeguarding Lead. Reports will be treated in confidence.

## Annex 1: ICT Acceptable Use Agreement

Dear Parents,

### ICT and E-SAFETY Policy

With this letter you will find a copy of our ICT and E-Safety Policy. This is a standard policy now being used by many schools and colleges, and I would ask you to read it carefully and to discuss it with your son/daughter. You will note that we are asking both you and your son/daughter to sign the document. Enclosed are two copies of the policy, one for you to keep and the other to be signed and returned.

The policy does look somewhat forbidding, but the intention is to ensure that pupils use our computer facilities, which includes access to the internet, sensibly and profitably. We want to ensure that pupils are not exposed to any inappropriate or unsuitable material and to this end the College filters all internet content. But despite careful design, filtering systems cannot be completely effective due to the speed of change and linked nature of Internet content and it is not possible to guarantee that unsuitable material will never appear on a College computer. Neither the College nor Astrum Education Ltd can accept liability for the material accessed or any consequences of Internet access. Pupils are encouraged to act responsibly and be aware when accessing internet content.

The College reserves the right to monitor, record and store a 'profile' of computing activities for anyone using the computer resources, and that this information may be used in evidence if considered necessary in the light of inappropriate, unethical or illegal activity. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

This document is being sent to parents and Guardians of children at CIC because we would like to encourage the pupils to make use of the computers during break time should they so wish. The signatures will imply permission for the time your son/daughter is at CIC. The aim and spirit of our ICT and E-SAFETY Policy will remain the same from year to year but we reserve the right to change the wording of some of the technical details in order to take account of any recent developments in ICT. We will keep pupils informed of any changes. Seminars on E-Safety and Safeguarding are also made available throughout the term to parents who wish to learn more information about the relative merits as well as hazards of the online world.

I hope that you will agree with the aims of this policy and will give your permission for your son/daughter to use the facility if he/she wishes. Please return the signed form to me as soon as possible.

Yours sincerely,

## PUPIL ICT ACCEPTABLE USE POLICY

Access to the College's computing facilities, which include the Internet, is provided for the purposes of educational research and learning. The purpose of this policy is to provide rules for its appropriate use. Pupils and parents are asked to read carefully and then sign the following agreement. If the signed agreement is not returned to the College, the pupil will not be allowed access to the College's computer facilities.

### Pupil Agreement

I understand that access to the computing facilities, which includes the internet, at CIC must be in support of educational research or learning, and I agree to the following:

- academic use takes priority at all times;
- I will keep my password secure and will only use a College computer whilst logged on with my correct username and password;
- I will not let others use my username and password and will not leave a computer whilst logged on;
- I will not tamper with files, passwords or other type of data or electronic media belonging to other users;
- the College reserves the right to monitor, record and store a 'profile' of computing activities for anyone using the network resources, and this information may be used in evidence if considered necessary in the light of inappropriate, unethical or illegal activity;
- the College's Internet service is filtered with the aim of preventing unsuitable material being accessed;
- I will refrain from accessing any newsgroups, links, list-servers, Web pages or other areas of cyberspace that would be considered as offensive by the College or my parents/guardians, because of pornographic, racist, violent, sexist, defamatory, blasphemous or other content and I am responsible for reporting these links if any appear inadvertently during my research;
- I will not use the Internet time in College for 'chat' programs and will not reveal any personal information of any type about others or myself;
- I accept that plagiarism is unacceptable, this includes copying material from other pupils and claiming it as my own work. I will respect copyright laws and intellectual property right when using resources from the Internet and I will not upload to or download from websites that encourage plagiarism or other academic dishonesty. I will only use downloaded materials in an appropriate manner in my work, listing it in a bibliography and clearly specifying directly quoted material;
- I will not attempt to install, store or use unauthorised copies of licensed or unlicensed software or use software that causes inconvenience to others;

- I will not store 'program' files or other 'executable' files or distribute them on the system or violate any network-related policy set by the College;

- I will not use College computer resources (including printers) in any way to aid with the illegal reproduction or selling of copyright material, including copies of CDs and DVDs;

- I will at all times act responsibly when using computer equipment, and take care not to physically damage ICT equipment. I understand that any wilful damage that I am responsible for, I will be expected to pay for;

- If I become aware of a suspected breach of data either through human error or malicious attack, I will notify the College GDPR Champion (Head of Computing) with immediate effect, and in any case within 24 hours.

***Email***

- College e-mails will be filtered for forbidden content and pupils may be blocked and disabled from using the system accordingly;

- I will be courteous and use appropriate language in any e-mail I may send to other users. I understand that the laws of libel and copyright may apply to e-mail;

- the College does not permit the sending or receiving of e-mail messages greater than a certain size (currently 2.5 MB including attachments) or the sending of e-mail multiple times or to multiple recipients. This is to prevent the transmission of uncompressed images and software, which can make unreasonable demands on network bandwidth and storage space.

**I realise that if I violate any of these terms I may be denied access to the College's computing facilities for a period of time to be determined by the College.**

Pupil Signature: …………………………………… Date: ………………….

Please print name: ………………………………. Year: …………………

**Parental Agreement**

As the parent/guardian of ……………………………………, I hereby acknowledge that I have read and understood the agreement on pupils' use of the College's computing facilities, which includes the Internet, and discussed it with him/her. I understand that access to the facilities is designed for educational purposes. I understand that the College will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the College cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the College is not liable for any damages arising from use of the Internet facilities.

**Parent/Guardian signature:………………………………..................**

**Please print name: ……………………………………… Date: …………….**