Copleston High School

Part of GIPPESWYK COMMUNITY EDUCATIONAL TRUST

Achieving success together

This Policy has been adopted and approved by Gippeswyk Community Educational Trust and has been adapted for use by Copleston High School.

ICT & ACCEPTABLE USE OF MOBILE PHONES POLICY	
Approved by GCET/Adapted by Copleston High School	1.9.2017
Reviewed/Amended	May 2021
Ratified by Copleston LGB	30.6.21
Date of next Review	Summer Term 2022
Responsible Officer	ICT Systems Manager
Policy Number	CS3

The need for a policy

All Copleston High School information communication technology (ICT) facilities and information resources remain the property of Copleston High School and not of particular individuals, teams or departments. By following this policy we will help ensure that ICT facilities are used:

- legally;
- securely;
- without undermining Copleston High School;
- effectively;
- in a spirit of co-operation, trust and consideration for others;
- so that they remain available.

The policy relates to all ICT facilities and services provided by Copleston High School, although special emphasis is placed on email and the internet. All employees, volunteers, and any other users of our IT are expected to adhere to the policy.

1. Disciplinary measures

1.1. Deliberate and serious breach of the policy statements in this section may lead to Copleston High School taking disciplinary measures in accordance with the disciplinary procedure policy. Copleston High School accepts that ICT – especially the internet and email system – is a valuable business tool. However, misuse of this facility can have a negative impact upon employees and volunteer productivity and the reputation of the organisation.

1.2. In addition, all of the organisation’s phone, internet and email related resources are provided for business purposes. Therefore, the organisation maintains the right to monitor the volume of internet and network traffic, together with the email systems. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

2. Security

2.1. As a user of Copleston High School’s equipment and services, you are responsible for your activity.

2.2. Do not disclose personal system passwords or other security details to other employees, volunteers, external agents and students. Do not use anyone else's log-in; this compromises the security of Copleston High School. If someone else gets to know your password, ensure that you change it or get the ICT support department to help you

2.3. If you intend to leave your PC or workstation unattended for any reason, you should lock the screen to prevent unauthorised access. If you fail to do this, you will be responsible for any misuse of it while you are away. Logging off is especially important where members of the public have access to the screen in your absence.

2.4. Do not attempt to gain unauthorised access to information or facilities. The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorised access to any computer (including workstations and PCs) or to modify its contents. If you do not have access to information or resources you feel you need, contact the ICT support department.

3. Use of Email

3.1. When to use email:

3.1.1. Use email in preference to paper to reach people quickly (saving time on photocopying / distribution) and to help reduce paper use.

3.1.2. Use the phone for urgent messages (email is a good backup in such instances). Use of email by employees and volunteers of Copleston High School is permitted and encouraged where such use supports the goals and objectives of Copleston High School.

3.1.3. However, Copleston High School has a policy for the use of email whereby employees and volunteers must ensure that they:

3.1.3.1. comply with current legislation;
3.1.3.2. use email in an acceptable way;
3.1.3.3. do not create unnecessary business risk to Copleston High School by their misuse of the internet.

3.2. Unacceptable behavior

3.2.1. Sending confidential information to external locations without appropriate safeguards in place. See paragraph 5 of this document for more details.

3.2.2. Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal.

3.2.3. Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment or bullying.

3.2.4. Using copyrighted information in a way that violates the copyright.

3.2.5. Breaking into Copleston High School's or another organisation's system, or unauthorised use of a password / mailbox.

3.2.6. Broadcasting unsolicited personal views on social, political, religious or other non-business related matters.

3.2.7. Transmitting unsolicited commercial or advertising material.

3.2.8. Undertaking deliberate activities that waste employee's effort or networked resources.

3.2.9. Deliberately or recklessly introducing any form of computer virus or malware into the corporate network.

3.3. Confidentiality

3.3.1. Always exercise caution when committing confidential information to email since the confidentiality of such material cannot be guaranteed. Copleston High School reserves the right to monitor electronic communications in accordance with applicable laws and policies. The right to monitor communications includes messages sent or received by system users (employees, volunteers and temporary employees) within and outside the system as well as deleted messages. Consider how the GDPR policy applies to this. See paragraph 5 for more detail.

3.4. General points on email use

3.4.1. When publishing or transmitting information externally be aware that you are representing Copleston High School and could be seen as speaking on Copleston High School's behalf. Make it clear when opinions are personal. If in doubt, consult your line manager;

3.4.2. Treat others with respect and in a way in which you would expect to be treated yourself (e.g. do not send unconstructive feedback, argue, or invite colleagues to make public their displeasure at the actions / decisions of a colleague);

3.4.3. Do not forward emails warning about viruses (they are invariably hoaxes and the ICT support department will probably already be aware of genuine viruses – if in doubt, contact them for advice);

3.4.4. Do not open an email unless you have a reasonably good expectation of what it contains, and do not download files unless they are from a trusted source. For example, do open **report.doc** from a colleague you know but do not open **explore.zip** sent from an address you have never heard of, however tempting. Alert ICT Support if you are sent anything like this unexpectedly.

3.5. Email signatures

3.5.1. Keep these short and include your name, title, phone / fax number(s) and website address.

4. Use of the Internet

4.1. Use of the Internet by employees and volunteers is permitted and encouraged where such use supports the goals and objectives of the school.

4.2. However, when using the Internet, employees and volunteers must ensure that they:

4.2.1. comply with current legislation;

4.2.2. use the internet in an acceptable way;

4.2.3. do not create unnecessary business risk to the organisation by their misuse of the internet.

4.3. Unacceptable behaviour

4.3.1. In particular the following is deemed unacceptable use or behaviour by employees and volunteers (this list is non-exhaustive):

4.3.1.1. Visiting internet sites that contain obscene, hateful, pornographic or other illegal material;

4.3.1.2. Using the computer to perpetrate any form of fraud, or software, film or music piracy;

4.3.1.3. Using the internet to send offensive or harassing material to other users;

4.3.1.4. Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence;

4.3.1.5. Hacking into unauthorised areas;

4.3.1.6. Creating or transmitting defamatory material;

4.3.1.7. Undertaking deliberate activities that waste employees effort or networked resources;

4.3.1.8. Deliberately or recklessly introducing any form of computer virus into Copleston High School's network.

4.4. Chat rooms / instant messaging (IM)

4.4.1. The use of chat rooms and instant messaging is permitted for business use only. This use must have been agreed with your line manager.

4.5. Personal Email

4.5.1. The use of personal email (e.g. Hotmail, GMail) is not permitted in the organisation unless previously agreed with your line manager.

4.6. Obscenities / pornography

4.6.1. Do not write, publish, look for, bookmark, access or download material that might be regarded as obscene or pornographic.

4.7. Copyright

4.7.1. Take care to use software legally and in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

4.7.2. Be aware of copyright law when using content you have found on other organisations' websites. The law is the same as it is for printed materials.

5. Confidentiality

5.1. If you are dealing with personal, sensitive and / or confidential information, then you must ensure that extra care is taken to protect the information. See Data Protection policy for more information.

5.2. If sending personal, sensitive and / or confidential information via email, then the following protocols should be used. If there is any doubt as to the information being sent or the appropriate level of protection required, please check with the data protection officer.

5.2.1. Personal, sensitive and / or confidential information should be contained in an attachment;

5.2.2. In appropriate cases the attachment should be encrypted, and / or password protected;

5.2.3. Any password or key must be sent separately;

5.2.4. Before sending the email, verify the recipient by checking the address, and if appropriate, telephoning the recipient to check and inform them that the email will be sent;

5.2.5. Do not refer to the information in the subject of the email.

5.2.6. Reference should be made to the Trust’s Data Protection Policy and references to the General Data Protection Regulations when handling and circulating ‘personal data’.

6. Copleston High School’s network

6.1. Keep master copies of important data on Copleston High School’s network server or in Office 365 and not solely on your PC's local C: Drive or portable disks. Not storing data on Copleston High School’s network server or in Office 365 means it will not be backed up and is therefore at risk.

6.2. Ask for advice from ICT support if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disk space very quickly and can impact network performance.

6.3. Be considerate about storing personal (non-Copleston High School) files on Copleston High School's network.

6.4. Do not copy files that are accessible centrally into your personal directory unless you have good reason (i.e. you intend to amend them or you need to reference them and the central copies are to be changed or deleted) since this uses up disk space unnecessarily.

7. Removable media

7.1. If storing or transferring personal, sensitive, confidential or classified information using Removable Media you must first contact the ICT support department for permission, but

7.1.1. Always consider if an alternative solution already exists, for example OneDrive;

7.1.2. Only use removable media provided by the ICT support department;

7.1.3. Encrypt and password protect;

7.1.4. Store all removable media securely;

7.1.5. Removable media must be disposed of securely by the ICT support department.

8. Personal use of ICT facilities

8.1. Social media

For the purposes of this policy, social media websites are web-based and mobile technologies which allow parties to communicate instantly with each other or to share data in a public forum. They include websites such as Facebook, Twitter, Instagram and LinkedIn. They also cover blogs and image sharing websites such as YouTube and Pintrest. This is not an exhaustive list and you should be aware that this is a constantly changing area.

8.1.1. Use of Social Media at work

8.1.1.1. Employees and volunteers are permitted to make reasonable and appropriate use of social media websites from Copleston High School's IT equipment. You should ensure that usage is not excessive and does not interfere with work duties. Use should be restricted to your non-working hours, unless this forms part of your work responsibilities.

8.1.1.2. Access to particular social media websites may be withdrawn in the case of misuse.

8.1.1.3. Inappropriate comments on social media websites can cause damage to the reputation of the organisation if a person is recognised as being an employee or volunteer. It is, therefore, imperative that you are respectful of the organisation's service as a whole including clients, colleagues, partners and competitors.

8.1.1.4. Employees and volunteers should not give the impression that they are representing, giving opinions or otherwise making statements on behalf of Copleston High School unless appropriately authorised to do so. Personal opinions must be acknowledged as such, and should not be represented in any way that might make them appear to be those of the organisation. Where appropriate, an explicit disclaimer should be included, for example: '*These statements and opinions are my own and not those of Copleston High School.'*

8.1.1.5. Any communications that employees or volunteers make in a personal capacity must not:

8.1.1.5.1. bring Copleston High School into disrepute, for example by criticising clients, colleagues or partner organisations;

8.1.1.5.2. breach Copleston High School's policy on client confidentiality or any other relevant policy;

8.1.1.5.3. breach copyright, for example by using someone else's images or written content without permission;

8.1.1.5.4. do anything which might be viewed as discriminatory against, or harassment towards, any individual, for example, by making offensive or derogatory comments relating to: age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation;

8.1.1.5.5. use social media to bully another individual;

8.1.1.5.6. post images that are discriminatory or offensive (or links to such content).

8.1.2. Copleston High School maintains the right to monitor usage where there is suspicion of improper use.

8.2. Other personal use

8.2.1. Use of facilities for leisure or personal purposes (e.g. sending and receiving personal email, personal phone calls, playing computer games and browsing the internet) is permitted so long as such use does not:

8.2.1.1. incur specific expenditure for Copleston High School;

8.2.1.2. impact on the performance of your job or role (this is a matter between each member of employees or volunteer and their line manager);

8.2.1.3. break the law;

8.2.1.4. bring Copleston High School into disrepute;

8.2.1.5. detrimentally affect the network performance by using large amounts of bandwidth (for instance by downloading / streaming of music or videos);

8.2.1.6. impact on the availability of resources needed (physical or network) for business use.

8.2.2. Any information contained within Copleston High School in any form is for use by the employee or volunteer for the duration of their period of work and should not be used in any way other than for proper business purposes, or transferred into any other format (e.g. loaded onto a memory stick / pen drive), unless necessary for business use, and with prior agreement of the line manager.

9. Portable and Mobile ICT Equipment

9.1. This section covers items such as laptops, mobile devices and removable data storage devices. Please refer to paragraph 7 of this document when considering storing or transferring personal or sensitive data. A separate Staff Mobile Phone Policy is available.

9.2. Use of any portable and mobile ICT equipment must be authorised by the ICT support department before use.

9.3. All activities carried out on Copleston High School's systems and hardware will be monitored in accordance with the general policy.

9.4. Employees and volunteers must ensure that all data belonging to Copleston High School is stored on Copleston High School's network and not kept solely on a laptop. Any equipment where personal data is likely to be stored must be encrypted.

9.5. Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of the car before starting your journey.

9.6. Synchronise all locally stored data, including diary entries, with the central organisation network server on a frequent basis.

9.7. Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.

9.8. The installation of any applications or software packages must be authorised by the ICT support department, fully licensed and only carried out by the ICT support department.

9.9. In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

9.10. Portable equipment must be transported in a protective case if one is supplied.

9.11. You are responsible for any software that you install on your machine, you should not install anything that isn't first approved by ICT and its source verified as legitimate.

10. Remote Access

10.1. If remote access is required, you must contact the ICT support department to set this up.

10.2. You are responsible for all activity via your remote access facility.

10.3. Laptops and mobile devices must have appropriate access protection, i.e. passwords and encryption, and must not be left unattended in public places.

10.4 To prevent unauthorised access to Copleston High School's systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone.

10.5. Select PINs that are not easily guessed, e.g. do not use your house or telephone number and do not choose consecutive or repeated numbers.

10.6. Avoid writing down or otherwise recording any network access information where possible. Any information that is written down must be kept in a secure place and disguised so that no other person is able to identify what it is.

10.7. Protect Copleston High School's information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-office environment.

10.8. Users of laptops and mobile devices are advised to check their car and home insurance policies for the level of cover in the event of equipment being stolen or damaged. Appropriate precautions should be taken to minimise risk of theft or damage.

10.9. Care should be taken when working on laptops in public places (e.g. trains) that any employee or client details are not visible to other people. For more info check the CHS data protection policy.

10 Electronic monitoring

10.1 Monitoring and logging of ICT use is in effect on all Copleston devices, this facility will only be used to appropriately protect Copleston and its interests and to help enforce or monitor other elements of this policy and the continued wellbeing of the network and related systems.

11 Online purchasing

11.1 Any users who place and pay for orders online using personal details do so at their own risk and Copleston High School accepts no liability if details are fraudulently obtained whilst the user is using Copleston High School's equipment.

12 Care of equipment

12.1 Do not rearrange the way in which equipment is plugged in (computers, power supplies, phones, network cabling, modems etc.) without first contacting the ICT support department.

13 Mobile phone communication and instant messaging

13.1 Staff are advised not to give their home telephone number or their mobile phone number to pupils. Mobile phone communication should be used sparingly and only when deemed necessary.

13.2 Staff are advised not to make use of pupils' mobile phone numbers either to make or receive phone calls or to send to or receive from pupils text messages other than for approved school business.

13.3 If mobile phone voice or text communication is established with a student because of educational necessity, the following guidelines must be followed:

13.3.1 The staff member's line manager must be informed in writing in advance.

13.3.2 Student's parents or guardians must be informed in writing in advance.

13.3.3 Photographs and videos of pupils should not be taken with mobile phones.

13.3.4 Photographs and videos of staff should not be taken with mobile phones.

13.4 Staff should only communicate electronically with pupils from school accounts on approved school business, e.g. coursework.

13.5 Staff should not enter into instant messaging communications with pupils.

13.6 Student's use of mobile telephones is restricted and the following rules MUST be followed:

13.6.1 Mobile phones are not to be used in the main school building during the school day

13.6.2 Mobile phones can only be used at break and lunch outside

13.6.3 Mobile phones will be confiscated by staff if used during prohibited times

13.6.4 Earphones must also be out of sight during the school day

13.6.5 Students must not photograph members of staff using their mobile phones or any other mobile device.

13.6.6 Students must not take photographs of each other if they could be used for any inappropriate purpose what so ever.

13.6.7 A confiscated mobile phone will be placed in a secure cabinet in the pastoral area and students can collect them at the end of the school day from a member of the pastoral team.

13.6.8 Students bring their mobile phone and any other electronic device to school at their own risk. We do not accept any responsibility for damage or theft of a mobile phone or other electronic device unless there is negligence on the school's behalf.

14 Wearable technology

14.1 Wearable technology is difficult to manage due to the nature of it always being on the wrist and could easily cause distraction within lessons. As such we have decided to not ban the technology however we strongly advise against bringing it in to the school because of the distractions it can cause. If wearable technology is worn the following points must be adhered to:

14.1.1 If wearable technology is worn it must be kept in a Do Not Disturb mode to prevent distraction.

14.1.2 Wearable technology is strictly prohibited during exams. Exam regulations do not allow this type of device and will result in disqualification if worn.

14.1.3 If these points are ignored and the wearable technology is causing a distraction the device can be confiscated until the end of the school day.

15 Agreement

All employees, volunteers, contractors or temporary employees who have been granted the right to use Copleston High School's ICT systems are required to sign this agreement confirming their understanding and acceptance of this policy.

Signed:		**Signed:**	

Manager:		**Employee [/volunteer]:**	
Date:		**Date:**	