ePolicy

The Policy contains two sections.

- **Section A: Device Usage Policy**
- **Section B: Social Media Policy**

Summary

The College's ePolicy deals with both the acceptable use of computers/mobile devices (referred to as "devices"),and the use of the internet, email and social media.

Full details of the policy are in the two sections that follow this summary. Everyone must read and comply with the full policy. Not doing so could result in disciplinary action. If you are at all unsure about anything in the ePolicy you should ask for clarification from your line manager, the IT Department or HR.

The main purposes of the policy are:

- To ensure full compliance with the General Data Protection Regulation ("GDPR");
- To ensure the security of the College's IT systems and hardware;
- To ensure that only properly licensed software and applications are used;
- To prevent illegal activities and bringing the College or individuals into disrepute;
- To prevent causing offence to students, their parents, other employees or anyone else;
- To ensure that everyone's use of College IT systems, the internet and social media is appropriate and legal.

The ePolicy applies whether you are using a College device or your own. The key points are:

1. You are responsible for the safe-keeping of any device you use.
2. Do not leave any device in a state in which it can be used without your knowledge by someone else.
3. Always use passwords which are not easy to guess, and keep them secret.
4. Make sure that all personal and confidential data are kept secure and cannot be either deliberately or accidentally accessed by anyone without authority.
5. Keep your data and documents backed up at all times. Make sure you know what is and is not automatically backed up.
6. Do not use software, applications or peripheral devices which have not been approved and installed by the IT Department.
7. Do not disable security or anti-virus devices or software.
8. During working hours, restrict the use of the internet and social media to College-related business, and under no circumstances access material which is offensive or illegal.
9. The College reserves the right to monitor employees' use of the internet during routine audits or when excessive, inappropriate or unauthorised use is suspected.
10. When using social media at any time, including outside work, do not make any postings which could cause offence to students, work colleagues or anyone else connected with the College, or which could directly or indirectly bring the College into disrepute, or lead to legal proceedings being taken against you or the College. You should be mindful that anything posted on the internet can be made public, whatever privacy settings are put in place.
11. As is also made clear in other College policies, use of IT systems, the internet, social media and email to communicate with current students must be restricted to College business and must never be of a personal nature.
12. Your College email account should be used only for College business.

13. Email accounts will not be routinely "trawled" but the College owns all communications sent by email and has the right to access material in your College email account and on College devices at any time.
14. All College devices and data must be returned when you leave St Clare's. You must also make sure that you have told your line manager the login details and passwords that they will need to access documents and data after you have left.

This is only a summary of the main points: the full requirements of the policy are set out in the sections which follow.

Section A: Device Usage Policy

1. Aim of the policy

In this policy, the term 'device usage' refers to the use of PCs, laptops, tablets, smartphones and other similar devices by members of staff while working for the College.

The aim of this policy is to ensure that computer usage at St. Clare's:

- complies fully with the law
- is secure
- is properly licensed
- does not result in the improper use of personal data
- does not bring individuals or the College into disrepute
- does not cause offence to colleagues or students
- does not negatively affect staff performance

Employees who use the College's computers inappropriately or excessively for personal and private purposes will be dealt with under the College's disciplinary procedure.

Intentional interference with the College's computer hardware, software or network, or the unauthorised use or sharing of personal data constitutes gross misconduct and may result in summary dismissal.

2. Security protocols

Because many computer files contain confidential or sensitive information, the College takes their security very seriously. For this reason employees must follow these basic security precautions:

a) Logging off

- Lock the screen if you leave your device for more than a couple of minutes
- Log off if you leave your device for a long period of time.
- Shut down completely any device that you have finished using at the end of each working day.

b) Device passwords

- Create a password using a mix of letters and numbers
- Do not use one that is obvious such as your date of birth or the name of a close family member
- Do not use personal passwords e.g. internet banking passwords
- Keep your password confidential; do not write it down and do not share it with anyone else (including other members of staff)
- Always change your password immediately if you suspect that someone knows it
- Notify your line manager immediately if you notice any suspicious activity, for example an employee or a student trying to gain unauthorised access to a computer.

c) Security tips

- Disconnect and lock up any security device (e.g. card reader) when you are not using it
- Ensure that you close your email folder when making a presentation to a group (e.g. agents, students etc.)
- Do not allow family members to use a College device

Please note: Temporary employees are issued with a generic ID and password which is changed once that person has left the College's employ.

3. Data protection and security

College devices and the data they contain are intended for business-related activities and for you to carry out your duties.

- Do not amend, delete, copy or take data off-site unless this is both specifically related to your work and you have the authority to do so. In particular, do not delete or amend any documents or programmes which are stored on the College's communal drives unless authorised to do so.
- Handle personal information in line with data protection principles (Data Protection Act 1998). Use only College computers when processing data that relates to living individuals, unless you have been given permission to use your own computer to carry out work-related duties e.g. a teacher who uses their own laptop for work. This includes creating any document or record in which people are named or can be identified.
- Use College devices on College premises, as far as is practicable. If you do use College devices at home, e.g. writing reports, preparing UCAS references and so on, every care must be made to protect this information by keeping it secure through the use of passwords and by physically keeping the laptop in a secure place. If a device or data is lost or stolen, tell your line manager and the Bursar immediately, in accordance with the College's Data Breaches Policy
- Ensure that data is secure at all times whether at College, at home, or if you take your device on a course or on holiday and during travel between those locations.
- Do not store non-work related data on College devices.
- Do not store any St Clare's data on third party cloud-based storage systems, other than those set up and approved in writing by the IT Manager.

4. Storage and Backup

Employees must work together with the IT department to ensure that all data is correctly stored and backed up:

- Store your data on the H-drive or other network shared drives, preferably in My Documents.
- Most data is backed up automatically every day
- Please note: the following data is **not** backed up:
    - the local C: or D: drives on your PC/laptop
    - very large files, such as Jpg, MP3
    - data on mobile devices

If this data is important, you should back it up yourself or, in the case of videos, burn on to CD or DVD. If in any doubt about the security of the St. Clare's data you must contact the IT department for advice.

5. Use of personal devices

Most employees have their own personal mobile devices such as smartphones, tablets and handheld computers. If these are used for work there is an increased risk for the College - in terms of the security of IT

networks and communications systems, the protection of personal data, confidential or sensitive business information, and compliance with legal obligations.

For these reasons, employees must always follow the security guidelines in this policy if they use a personal mobile device for work-related purposes.

- Password protect the device, using biometric security functions if the device supports them.
- Use a tracking app to allow the device to be found and data erased remotely.
- Protect the data from family, friends or members of the public.
- Make available to the College via its own resources any data that belongs to St Clare's and is essential to its business.
- Remove all College data when you cease employment with St Clare's.

The IT department has absolute discretion to reject a device or refuse or revoke permission for a particular device. In order to access the College's systems the IT department may need to install software applications on the device. If any such software is removed, access to the College's systems will be disabled.

You must report any lost, stolen or compromised personal device to the IT department immediately (Data Breaches Policy). In these circumstances the College will probably erasethe data remotely and this may destroy not only College data but also your own data since it is not always possible to distinguish between the two.

You must erase all College data from a device before you upgrade to a new device and/or sell it.

6. Use of portable storage devices

Some employees may use portable storage devices, such as memory sticks and portable hard drives. However, their small size and storage capacity makes them vulnerable to misuse or loss. If you use a portable storage device you must:

- password protect the data on any portable storage device
- get approval from the IT Manager before using a portable storage device.
- never transfer data to a third party computer (including one at home)
- report the loss of any portable storage device immediately to the IT Manager and the Bursar (Data Breaches Policy)
- observe any guidelines which may be introduced from time to time.

7. Software

The College does not own any computer software: it is licensed to use the software from a variety of outside companies.

- Do not reproduce software, or infringe copyright in any way, without the express permission of the software developer. Contravention is a disciplinary matter and will be dealt with in accordance with the College's disciplinary procedure.
- Use only software supplied and approved by the IT Department. If you need non-standard software, you must complete the appropriate form, obtain approval from your line manager, and return it to the IT Manager. Approval may also be needed from the College’s Information Systems Steering Group. The software will be added to the Asset Database and made available to the user on their device.
- New software must be obtained and installed by IT staff unless previously agreed with the IT department which must keep proof of purchase. N.B. this includes all shareware, freeware and public domain software. The unauthorised installation of software onto College devices may result in disciplinary action.

8. Viruses

The College's computer network remains vulnerable to viruses even though virus protection software is installed and automatically updated. Re-configuring or disabling this software is prohibited and may result in disciplinary action.

If your computer starts to behave 'strangely' or you suspect it may have become infected with a virus, turn it off immediately and contact the IT department.

The College undertakes both random and targeted testing of employees' awareness of potential phishing attacks. Concerns about individual or collective awareness will result in compulsory additional training being given.

9. Games

You must not install games onto College devices. Employees may only play computer games on their own devices outside their working hours.

10. Remote access

Any employee who works remotely should be aware that all aspects of this policy apply at all times.

- Do not allow family members or other third parties to use the College's devices (including software) or to access or view its internal IT networks.
- Observe any additional guidelines that may be introduced to reduce the likelihood of the College's computer networks being compromised as a result of remote access.

11. Email and other electronic communications

St. Clare's is an open, tolerant community and there is an implicit assumption that employees will not send emails/texts which are likely to be considered offensive and/or discriminatory, e.g. relating to race, gender, age, nationality, religion and so on (see also the Code of Conduct and the Equal Opportunities & Dignity at Work Policies). The sending of such emails would be dealt with under the College's Disciplinary Procedure.

You must:

- use your St. Clare's email address for communicating with current students whenever possible.
- only use St. Clare's email accounts for personal communication when this is absolutely necessary.
- never use personal email accounts for communicating on behalf of St. Clare's with current students, staff, clients or others.

The College will not routinely monitor the email accounts of its employees, but any communication sent by email/text or stored on College equipment is owned by St. Clare's. You should not think that your electronic communication or storage is private.

The College will only monitor and record any use that you make of our systems where we have a lawful basis for doing so. This will normally be where we need to do so to perform your employment contract, we need to comply with a legal obligation, or where such monitoring is necessary for our legitimate interests (and your interests or your fundamental rights and freedoms do not override our interests).

The business purposes for such monitoring, which confirms our legitimate interests, are to:

- establish the existence of facts, e.g. in response to a client or customer complaint
- ascertain compliance with regulatory or self-regulatory requirements, practices or procedures
- assess your standards of performance and conduct and promote productivity and efficiency
- investigate or detect any unauthorised use of the systems
- ensure the security of the systems and networks and their effective operation
- ensure the smooth running of the business by checking whether there are any relevant business communications that need to be dealt with, e.g. if you are absent for any reason
- ensure that the College's rules, policies and procedures are being complied with
- record transactions
- promote client and customer satisfaction
- ensure that the systems are not being used for any unlawful purpose or activities that may damage the College's business or reputation
- make sure there is no unauthorised use of the College's time, e.g. if you have been sending and receiving an excessive number of personal communications or spending an excessive amount of time viewing websites that are not work related
- perform effective internal administration
- ensure that inappropriate, restricted or blocked websites are not being accessed and that offensive or illegal material is not being viewed, sent, downloaded or circulated
- ensure that all employees are treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to unlawful harassment
- protect the privacy of personal data, trade secrets and sensitive or confidential College information and ensure there is no breach of confidentiality or data protection provisions.

12. Websites

Employees must ensure that they always use the internet in an appropriate and acceptable way.

- Do not visit internet sites that contain material which is obscene, pornographic, hateful, defamatory or promotes terrorism, drug use or any other illegal activity.
- Internet sites relating to alcohol and gambling must also not be visited. If you have a sound reason for needed to access such sites (such as for teaching purposes) you must ask your department head to request access on your behalf.
- If you inadvertently visit such a site, report the matter to IT immediately. Failure to do so could result in disciplinary action and/or could lead to police investigation.

Employees are also responsible for ensuring that third parties (including friends and family) do not use either College devices or the College's networks to access such inappropriate or unacceptable material on the internet.

13. Temporary workers

From time to time, the College appoints temporary staff and allows them access to the computer systems. In these cases it is the responsibility of the line manager:

- to bring this policy and its contents to their attention
- to identify any directories or computer files that are sensitive or confidential
- to inform the IT department and arrange restricted access as appropriate.

14. Auditing

The College uses auditing software to check whether software loaded onto College devices is legal. If a user contravenes this policy, IT will recall the device for inspection. The software could be removed and the employee could face disciplinary action.

The College uses software to restrict access to a range of websites (including those detailed in the 'Websites' section above). That software also monitors website usage and records attempts to access sites which are prohibited. If

15. The Asset Register

You must complete a loan form if you are issued with a College computer or tablet. If you change jobs within the College or move to another office/work station, you must inform IT so that software can be removed/updated and the Asset Register kept up to date.

16. Leaving St. Clare's

Your computer accounts will be disabled on your last day of work at College. All College devices (laptops, tablets, mobile phones etc.) must be handed to the IT department one day before you leave.

17. Contravention of this policy

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in action being taken under the College's disciplinary procedure.

Section B: Social Media Policy

1. Social media definition

Social media allow users to communicate instantly with each other or to share data in a public forum. They include

- social and business networking websites/apps such as Facebook, WhatsApp, MySpace, Weibo, Twitter and LinkedIn;
- video and image sharing websites/apps such as YouTube, Instagram, SnapChat and Flickr;
- personal blogs etc.

This is a constantly changing area with new services being launched on a regular basis and therefore this list is not exhaustive. This policy applies to any social media that employees may use.

2. Personal use of social media at work

Employees are only permitted to log on to social media websites, or to keep a blog, outside their normal working hours (for example, during lunch breaks or after their working day has finished). However, employees may be asked to contribute to the College's own social media activities during normal working hours, for example by writing College blogs or newsfeeds, managing a Facebook account or running an official Twitter or LinkedIn account for the College. Employees must be aware at all times that while contributing to the College's social media activities they are representing the College.

3. College's social media activities

If you are authorised to contribute to the College's own social media activities as part of your work, for example for marketing, promotional and recruitment purposes, you must follow these rules:

- use the same safeguards as you would with any other type of communication about the College that is in the public domain
- ensure that any communication has a purpose and a benefit for the College
- obtain permission from your line manager before embarking on a public campaign using social media
- follow any additional guidelines given by the College from time to time

The social media rules set out below also apply as appropriate.

In addition, social media accounts (and their contents) which are operated for business purposes belong to the College and must not be used after your employment has ended.

4. Social media rules

Many employees make use of social media in a personal capacity outside the workplace and outside normal working hours. While they are not acting on behalf of the College in these circumstances, employees must be aware that they can still cause damage to the College if they are recognised online as being one of its employees. Therefore, it is important that the College has strict social media rules in place to protect its position.

When logging on to and using social media websites and blogs at any time, including personal use on non-College computers outside the workplace and outside normal working hours, you **must not**:

- conduct yourself in a way that is potentially detrimental to the College or could bring the College or its employees, students, parents, agents, contractors or suppliers into disrepute, for example by posting images or video clips that are inappropriate or links to inappropriate website content
- use your work e-mail address when registering on sites or provide any link to the Colleges website (other than in relation to the College's own social media activities or where expressly permitted by the College on business networking websites such as LinkedIn)
- post messages on these websites or blogs that could damage working relationships with or between employees and students, parents, agents, contractors or suppliers of the College
- include personal information or data (including images) about the College's employees, students, parents, agents, contractors or suppliers without their express consent; this could constitute a breach of the General Data Protection Regulation and the UK Data Protection Act 2018 which is a criminal offence. An employee may still be personally liable even if employees, students, parents, agents, contractors or suppliers are not expressly named in the websites or blogs as long as the College reasonably believes they are identifiable
- make any derogatory, offensive, untrue, negative, critical or defamatory comments
- make any comments or post any images or video clips that could constitute unlawful discrimination, harassment or cyber-bullying
- disclose any trade secrets or confidential, proprietary or sensitive information that could be used by one or more of the College's competitors
- breach copyright, for example by using someone else's images or written content without permission or failing to give acknowledgement where permission has been given to reproduce particular work. If you wish to post images, photographs or videos of others on your online profile, you should first obtain the other party's express permission to do so
- You must not have current students as 'friends' on social networking sites, unless there are educational reasons for doing so; for example, a teacher might set up a Facebook account for use by students in a particular class.

Employees must immediately remove any content which does not comply with these rules, if they are asked to do so by the College.

On the termination of employment or whenever so requested by the College, you must give your line manager all login and password details for accounts run on the College's behalf or where an account has been used to promote and/or market the College's business activities.

You should remember that social media websites are public, even if you have set your account privacy settings at a restricted access or "friends only" level. You should not assume that your postings on any website will remain private.

You must also be security conscious when using social media websites and should take appropriate steps to protect yourself from identity theft, for example by placing your privacy settings at a high level and restricting the amount of personal information you give out, e.g. date and place of birth. This type of information may form the basis of security questions and/or passwords on other websites, such as online banking.

Should you notice any inaccurate information about the College online, you should report this to your line manager in the first instance.

5. Social media monitoring

The College reserves the right to monitor its employees' use of the Internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected.

The College reserves the right to restrict, deny or remove Internet access, or access to particular social media websites, to or from any employee.

6. Contravention of this policy

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under the College's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal.

Most recent review and/or amendment

SMG May 2018