St. Joseph's Specialist School & College
& Supported Living
Amlets Lane, Cranleigh
Surrey, GU6 7DH

Website: www.st-josephscranleigh.surrey.sch.uk

Internet & Electronic Media Acceptable Use Policy (Staff)

Christ in our Lives
'No limits ... just possibilities'

Your Life ... Your Way

Reviewed: July 2018
Care, Health & Safety Committee
3 yearly

WEBSITE POLICY

Contents

The Aims of the Policy

The policy is applicable to St. Joseph's Specialist School and College and to Springvale/Long Barn Supported Living; for the purposes of this policy these parties are now referred to as "St Joseph's".

For the purposes of this policy the term "staff" includes any adults that are working with students: teachers, teaching assistants, care staff and other helpers both paid and unpaid.

This policy aims to help staff with the following:

- To help adults that work with students to do so safely and responsibly when using the internet and electronic media.
- To clarify which behaviours constitute safe practice and which types of behaviour should be avoided by staff.
- To help staff understand the boundaries of acceptable behaviour.
- To support school managers and leaders in establishing: policies, codes of behaviour and a workplace ethos that safeguards staff as well as young people in the organisation.
- To assist school management teams in giving a clear message that unsafe or unlawful behaviour is unacceptable and that where appropriate, disciplinary or legal action will be taken.
- To support staff in their use of the Internet.
- To reduce the risk of staff inadvertently behaving in an inappropriate or illegal manner when using the Internet.
- To reduce the risk of unfounded allegations of inappropriate behaviour.

Staff will be provided with a copy of this policy which they must sign to confirm that they have read and understand it, and agree to abide by its terms.

Internet Access

You must not access or attempt to access any sites that contain or promote any of the following:

- child abuse
- pornography
- discrimination of any kind
- racial or religious hatred
- illegal acts
- provide information which may be illegal or offensive to colleagues.

Inadvertent access must be treated as a safeguarding incident and reported to the safeguarding team.

Social Networking

Social networking is allowed in school in accordance with this policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks.

Use of Email

Staff are not permitted to use school email addresses for personal business.

Staff must not send emails that are indecent, offensive or threatening. All email should be kept professional.

Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords

Devices that store personal information should be protected by secure passwords containing a combination of numbers, capitals and symbols. Passwords must never be left blank or at default.

In order to protect data on unattended equipment staff should ensure the device has an automatic timeout that requires a password after a short time period.

Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Data Protection

Any information that can be identified as relating to a named, living individual such as name, age, sex, attendance records etc. is classed as “personal information”. All personal information is subject to the Data Protection Act (DPA).

The DPA requires that personal data, in whatever form, is kept secure by the school, and, therefore, by all staff.

If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB Pendrive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT

You are not permitted to use ICT equipment for personal use unless specific permission has been given by the Executive Principal who will set the boundaries of such use.

Images & Videos

You should not upload onto any internet site or service images or videos of staff or pupils, or livestream or transmit in anyway without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Staff must avoid using personal phones or cameras and use school devices wherever possible. Images should be removed as soon as is practically possible should a personal device be used.

Images or videos should never be taken of students when they are in crisis unless approved by a member of the Senior Leadership Team and the family of the student. Videos of students in crisis should be treated as confidential personal information and, in accordance with the DPA, should only be stored for as long as is absolutely necessary.

Use of Personal ICT

Use of personal ICT equipment is at the discretion of the Executive Principal.

Viruses & other Malware

Any virus outbreaks are to be reported to the ICT Manager as soon as it is practical to do so.

E-Safety

Like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with students.

Responsibility for Electronic Devices

Staff are solely responsible for content accessed on school electronic devices when they are offsite. Therefore staff must ensure that they have absolute control of any school electronic device and its use when it is allocated to them.

The individual staff member is directly accountable for any content accessed or stored on the device. In the event that malicious software, illegal content or explicit material have been found to have been viewed or stored on a school device this would lead to disciplinary action and/or reporting to the police.

Communicating with students and their families

The DCSF stated in 2007 that:

"Communication between adults and students, by whatever method, should take place within clear and explicit professional boundaries. Adults should not share any personal information with the child or young person. They should not request, or respond to, any personal information from the child / young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny."

Staff should limit contact with young people and their families to official channels of communication. Currently St Joseph's Specialist School and College only officially recognise three forms of electronic communication:

- organisational email addresses ending with the domain:
- '@st-josephscranleigh.surrey.sch.uk'
- Information posted on the school website:
- 'www.st-josephscranleigh.surrey.sch.uk'
- Telephone

Any other form of electronic communication is considered unofficial and therefore a breach of this policy.

Staff must not give their personal e-mail addresses to young people to allow access outside of school hours.

Communicating with students and their families

Staff should not use their own mobile or home phones to communicate with students at any time.

It is inadvisable for staff members to use their own mobile phones to communicate with a student's family. Staff members should use the school landline when onsite and ensure they take a school mobile phone with them when out on visits.

I have read and understand the Internet & Electronic Media Acceptable Use Policy (Staff) and agree to abide by its terms.

Name:_____

Signature: _____

Date: _____

Date Policy Reviewed

Updated	Changes	By	Version
September 2010	Policy rewritten	Lucy Mayle / Simon Charleton	v1
September 2014	Minor amendments made ahead of full revision	Tom Milson	v1.1
March 2015	Full revision – version 2.0 made in light of the developments of technology and the implementation of additional electronic devices on site.	Tom Milson	V2.0
September 2015	Prevent duty added	Alan Day	V2.1
September 2017	Complete rewrite	Fairley Allan	V3
June 2018	Added section on images and videos including livestreaming.	Fairley Allan	V3.1