St. Joseph's Specialist Trust
Amlets Lane, Cranleigh
Surrey, GU6 7DH

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

Electronic & Social Media Guidelines

Christ in our Lives
'No limits … just possibilities'

Your Life ... Your Way

Last Reviewed: May 2024
Next Review: May 2025
Cycle: Annual

WEBSITE GUIDELINES

Contents

The Aims of these Guidelines

St. Joseph’s Specialist Trust comprises of a specialist school, college, registered children’s home and supported living function, together “St Joseph’s”. These guidelines apply to all members of the St Joseph’s community who have access to and are users of St Joseph’s ICT systems, both in and out of school.

For the purposes of these guidelines, the term “staff” includes any adults that are working with young people: teachers, teaching assistants, care staff and other helpers both paid and unpaid. The term “young people” includes students, residential students and tenants.

These guidelines are designed to be read in conjunction with the Safeguarding Policy and Anti-Bullying Policy.

Guidelines scope

These guidelines set out St Joseph’s approach to keeping young people safe with technology while at St Joseph’s and details staff responsibility around social media, use of the internet, mobile devices and IT equipment.

These guidelines also outline a code of conduct for staff to ensure their practice in their personal life does not spill over to affect their professional life.

It is recognised that young people at St Joseph’s are generally able to access the internet, social media and mobile devices, often with a degree of independence and therefore can be more at risk when using technology in their home environment as the technical support and protective measures available in the school environment may not be available at home, be that the family home or the children’s home (hereafter “home”). Therefore, these guidelines outline how young people can be supported to understand the potential risks.

These guidelines aim to help staff with the following:

- To help adults that work with young people to do so safely and responsibly when using the internet, mobile devices and electronic media.
- To clarify which behaviours constitute safe practice, which behaviours should be avoided and the boundaries of acceptable behaviour by staff.
- To support school managers and leaders in establishing policies, codes of practice and a workplace ethos that safeguard St Joseph’s staff as well as young people
- To give 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

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school 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 these guidelines, which may take place out of school, but is linked to membership of the school.

St Joseph's will deal with such incidents within these guidelines and associated behaviour and anti-bullying policies and will, where known, inform families / carers of incidents of inappropriate e-safety behaviour that take place out of school. This is overseen by the Headteacher and Head of Safeguarding.

Internet Access

Staff and young people 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 Media

The term social media refers to websites and applications that enable users to create and share content to participate in social networking.

The use of social media at St. Joseph's is allowed in accordance with these guidelines only. Staff using social media for personal use should never undermine the school, college, children's home, supported living function, its stakeholders, staff, parents, children or any other aspect of St Joseph's. Staff should not become "friends" with parents or pupils on personal social networks.

What are the particular risks around social media?

While developing technology brings many benefits it also has considerable risks. These include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to/loss of/sharing of personal information.
- The risk of vulnerable young people in particular being targeted for grooming by those with whom they make contact on the internet. Grooming can be defined as being befriended in order to take advantage of the person in some way. See the Safeguarding Policy for further details.

- The sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying – including persistent derogatory comments being made.
- The potential for excessive use which may impact on social and emotional development and learning.

Staff responsibilities for young people use of social media

- When using digital images, staff should inform and educate young people 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.
- Young people must be informed that they cannot take, use, share, publish or distribute images of others without their permission.
- Young people to be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Young people to be informed not to use their full names anywhere on a website or blog and never in association with photographs.
- Young people to be informed that they cannot use social networking technology to contact staff.
- A planned e-safety programme should be provided as part of ICT, PHSE and other lessons and should be regularly revisited, this will cover the use of ICT and new technologies in and outside school. For tenants staff should support the tenants to ensure their own e-safety in conjunction with the tenants' families where appropriate.
- Key e-safety messages should be reinforced through further input via assemblies in school and pastoral activities as well as informal conversations when the opportunity arises as well as through safe internet activities across the whole St Joseph's function.
- Staff must take steps to prevent young people publishing their contact details. If staff become aware that a young person has done so this must be immediately reported to Safeguarding.

Staff responsibilities in relation to staff's own use of social media

- Staff must not add young people as friends on their personal accounts, see the policy on Safeguarding.
- Staff must not identify themselves as connected with St Joseph's Specialist Trust except for on professional networking sites such as Linked In.
- Staff must not create, copy, share, distribute, publish or re- publish any information which may be offensive to stakeholders, colleagues, students, tenants or families or which breaches the integrity of the ethos of St Joseph's or brings St Joseph's into disrepute.

- Staff must not comment or allow any of their comments about any aspect of St Joseph's to be published in any press or online in any medium.
- Staff must take all reasonable precautions with security settings to ensure that private information remains private.
- Staff must not set up St Joseph's related sites, groups, pages or accounts without getting prior approval from the Executive Principal.
- Staff have a duty to report to the Executive Principal if anything is seen on social media sites which is a cause of concern in relation to any aspect of St Joseph's or anyone associated with it.
- Staff need to be aware that some images are copyright protected and so cannot be uploaded, shared or used in any other way. Staff must own images they intend to use or have express have permission to share such. Once an image is uploaded to a website it can be used and downloaded by others. On sites such as Facebook a published photograph no longer belongs exclusively to the person who published it and the site acquires a non- exclusive right to use such images or information.
- Staff must be personally responsible for content published into social media tools and aware that what is published will be public for many years.
- Staff are advised to avoid publishing personal contact details where they can be accessed and used widely.

Guidance for managing suspected on-line incidents involving social media

The following is intended for use when St Joseph's needs to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Examples of where this guidance is followed could be in cases of cyber-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites or blogs and so on.

- More than one senior staff member is involved in the process.
- The procedure is conducted using a designated computer that is not being used by young people and if necessary, can be taken from site by the police. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in cases of indecent images).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include:
    - Internal response or disciplinary procedures
    - Involvement by Local Authority or national/local organisation (as relevant)
    - Police involvement and / or action

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 emails must be kept professional.

St Joseph's 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. Staff should keep passwords private with the exception of the Safeguarding team, IT Support and Admin where group passwords have been set up as access is needed by all members of the group but should not be shared with anyone external from that group.

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 St Joseph's and, therefore, by all staff.

If it is necessary for staff to take work home, or off site, they should ensure that their device is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of St Joseph's ICT

Staff 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

Staff should not upload onto any internet site or service, images or videos of staff or young people, or livestream or publish or transmit in anyway without consent. This is applicable professionally (in any part of the St Joseph's operation) or personally (i.e. during staff outings or social gatherings).

Staff must avoid using personal phones or cameras and use St Joseph's devices wherever possible. Images should be removed as soon as is practically possible should a personal device need to be used in the course of work for St Joseph's.

Images or videos should never be taken of young people when they are in crisis unless for a pertinent reason and approved by a member of the Senior Leadership Team and the family of the student. Videos of young people 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 Head of ICT Manager or Deputy Head of ICT as a matter of urgency.

E-Safety

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

Responsibility for Electronic Devices

Staff are solely responsible for content accessed on St Joseph’s electronic devices when they are offsite. Therefore, staff must ensure that they have absolute control of any such 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 St Joseph’s device this would lead to disciplinary action and/or reporting to the police.

Communicating with young people and their families

The Department for children, Schools and families stated in 2007 that:

“Communication between adults and young people, 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 Trust 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 these guidelines.

Staff must not give their personal e-mail addresses to young people.

Communicating with young people and their families

Staff should not use their own mobile or home phones to communicate with young people 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.

Date Guidelines 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
January 2019	Minor change to Trust	Alan Day	V3.2
February 2020	Interim review to reclassify from Policy to Guidelines and cycle changed to annual	Admin	N/A
Summer 2020	Merged Social Media Guidelines into Internet & Electronic Media Acceptable Use Guidelines (staff) and renamed: Electronic & Social Media Guidelines.	Fairley Allan	V4
Summer 2021	Minor updates and changes. Change ‘students’ to ‘young people to include supported living tenants’	Fairley Allan	V4.1
March 2023	Various changes	Lizzie Hurst	V4.2
March 2023	Addition to anti-bullying paragraph	Simon Jaggard	V4.3
April 2023	Addition about shared emails	Nick Durling	V4.4
May 2024	No Changes	Lizzie Hurst	V4.5