ST JOSEPH'S CATHOLIC HIGH SCHOOL

ICT SAFETY AND ESAFETY

Part 2 – Use of Emails

Date of Review October 2018
Due for Review October 2020

Policy concerning ICT safety and e-Safety (including email, photography and text messaging)

The purpose of this document is to update our existing policies and practices and consolidate them into one document for ease of use and accessibility. The key documents that this document has been written include SSCB's *Guidance on The use of Email and Text messaging for professionals*, *Guidance using Images of Children: Photographs, Videos, Websites and Webcams* , OFSTED's *The Safe Use of New Technologies* (2010) and *School Evaluation: A response to the Byron Review* (2008). This policy reflects the guidance in those documents and seeks to draw its fundamental principles on safety into our school community. This document consists of 4 parts.

Part 2
Use of Emails

All emails relating to a parental communication must be retained and kept on the student's file. Emails must be regarded as correspondence and must be retained with other letters and faxes and retained in chronological order in the relevant section of the file[1]. When emails are printed it is important that the computer system is configured to print out details such as; sender, addressee and date sent, in order that a record of these details is kept[2].

EMAIL SECURITY

Internal emails

It is permitted to send emails containing personal-identifiable information[3] internally as this is a secure internal network. Staff are advised to apply the best practice guidance detailed below to all emails sent internally, as appropriate.

Emails Sent Externally

It is not advisable that sensitive, personal or confidential information should be sent by email to an external email address. It is permitted to send emails externally, providing all personal identifiers (e.g. name, address date of birth) are removed. It is suggested that the sender telephones the recipient of the email to pass on the necessary relevant identifiable information. If, in exceptional circumstances it is professionally considered to be essential for an email containing person identifiable information to be sent

[1] All agencies need to be able to identify than an email was sent and received on a certain date and the contents of that email. Therefore, the original email must be held on file to ensure that the document may be disclosed if required in the future.

[2] Disclosure covers documents that are or have been in the party's control and therefore the fact that the document was in electronic format does not remove the obligation to disclose, even if the email has been deleted. If the document has been destroyed, an application could be made to search the servers or hard drives of a party's computer to access deleted emails.

[3] Emails containing personal data must be processed in line with the Data Protection Act. As such they are liable to be disclosed under any client access to their personal data, for which each agency has their own procedure.

externally and it is impossible to remove all personal identifiers, then the best practice guidance detailed below must be followed.

Confirmation of Receipt of Emails

It is recommended that the return receipt function should be used in respect of all communications to a specific parent/agency.

Signposting of Emails

As for other correspondence, an entry should be made in the case record stating the date and time the email was sent or received.

Reports contained in attachments

Where emails are used to forward reports or documents[4] in an attachment, as an alternative to the postal service or internal mail, it is not necessary to retain the email once receipt of the report is obtained. It is necessary to make a brief record on the file of the method and date the report was forwarded and the date of receipt of the report.

Disclaimer

The school's disclaimer footnote should be automatically added to the bottom of all external emails.

GUIDANCE REGARDING THE CONTENT OF EMAILS

Each email must contain reference only to the individual or family concerned, as would normally be the case in respect of a letter. It should not contain information about other unrelated individuals or families. Jokes, asides and references to any matters not pertinent to the particular case should not occur.

Language of style of emails

All emails relating to users and/or their carers must be recorded as formal communications. As emails will form part of a case record, it is important that staff follow the guidance on recording and note that the language style should be:

- Clear, brief and objective
- In plain language
- Jargon free
- Correctly spelt
- Compiled as if all recordings will be read by the client

[4] A document is defined by the Civil Procedures Rules (R31.4) as *anything in which information of any description is recorded.* An email is a document that is transferred by electronic means, as opposed to by post or fax, and the method of transfer does not change the fundamental nature of the document.

BEST PRACTICE RE. THE USE OF EMAILS

Regarding emails sent internally; these best practice recommendations are for use where they consider it is appropriate, or necessary to do so. Use a return receipt function to see who has read the email and when received.

Regarding emails sent externally – all staff must follow these guidelines when sending emails externally:

- Ensure that there is no other person-identifiable information in the email
- Where person-identifiable information cannot totally be removed, or where the removal of the person-identifiable information does not remove by email the confidentiality of the information being sent (e.g. minutes of a strategy meeting), professionals must consider whether it is essential for this information to be sent by emails. If it is essential, professionals must ensure that the information sent has as much person-identifiable information removed as is reasonably practical and it is placed in an attachment rather than being in line text The attachment should be password protected, using a password that contains letters, numbers and symbols and is not an easily identifiable word. This password should then be given to the recipient. Always double check that the email address is correct.

All staff are advised to only communicate to students by the schools' social network (school email, school Twitter account etc.). Staff should never communicate to students via their own personal social media sites such as Facebook.