



Bishop Vesey's Grammar School:

Managing e-mail

This school seeks to do the following in regard to managing email:

- Manage accounts effectively with up to date account details of users.
- Report messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Know that spam, phishing, virus, Trojans and malware attachments as well as inappropriate language or material based messages can make e mails dangerous. We use a number of BGfL-provided technologies to help protect users and systems from the significant risks. In school desktop anti-virus product Sophos is installed on every client. BGfL provides Clearswift MIME Sweeper for email content filtering and McAfee Webwasher filtering monitors and protects our internet access to the World Wide Web.

Pupils:

- Pupils' e-mail accounts within school are intentionally 'anonymised' for their protection.
- Pupils are introduced to, and use e-mail as part of a scheme of work in Year 7 and through form periods focused on aspects of e-safety throughout the year.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
 - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
 - that an e-mail is a form of publishing where the message should be clear, short and concise;
 - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
 - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
 - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
 - that they should think carefully before sending any attachments;

- embedding adverts is not allowed;
 - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
 - not to respond to malicious or threatening messages;
 - not to delete malicious offensive threatening e-mails, but to keep them as evidence of bullying;
 - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
 - that forwarding 'chain' e-mail letters is not permitted.
- Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff can only use the Bishop Vesey's Grammar School email systems on the school system
- Staff only use Bishop Vesey's Grammar School email systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Never use email to transfer staff or pupil personal data.
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
 - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
 - the sending of chain letters is not permitted;
 - embedding adverts is not allowed;
- All staff sign our school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

- **Appendix 1 – further information**

- **How will e-mail be managed?**

- E-mail is now an essential means of communication for staff in schools and everyday life. Directed use of regulated e-mail in schools can bring significant educational benefits, increases the ease of communication with parents and within the school community and facilitates local and international school projects. However, e-mail can provide a means of access to a pupil that bypasses the traditional school physical boundaries. The central question is the degree of responsibility for self-regulation that may be delegated to an

individual. Use of freely available, unregulated email within a school is not appropriate.

- **Technology:**

- Spam, phishing and virus attachments are all potential risks to be considered. Filtering software must be used to stop unsuitable mail. BGfL's filtering provision is highly efficient in this respect, although it should be stressed that the technology only forms part of the protection strategy and should not be relied upon in isolation. Instead, it should be used alongside good classroom and supervisory practices, user education, and diligent individual behaviour.
- Regulated email is filtered and accountable. Use may also be restricted to approved addresses and filtered for unsuitable content and viruses. This is the first line of defence. Schools in Birmingham, have appropriate educational, filtered Internet-based e-mail options through the Birmingham Grid for Learning (BGfL).

- **Procedures:**

- In the school context, e-mail should not be considered private and most schools, and indeed Councils and businesses, reserve the right to monitor e-mail. There is a balance to be achieved between monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.
- The use of personal e-mail addresses for professional purposes, such as Hotmail, must be avoided by all staff working in schools. Staff should be required to use the appropriate Microsoft Exchange account provided by the school for professional purposes.
- Many teenagers will have their own e-mail accounts, such as the web-based Hotmail or G-mail, which they use widely outside school, usually for social purposes. These should not be used for school purposes. Where e-mail accounts are not monitored, there is the risk that pupils could send or receive inappropriate material.
- Email must not be used by staff to transfer information about pupils – unless it is within an encrypted, secured email system, approved and deemed appropriate for such use by your Local Authority. It is worth knowing that the data (in emails or other systems) does not belong to the User but to the organisation and they are not authorised to do as they please with the organisation's data. Therefore a school user could be personally liable for breaching the Data Protection Act (DPA98) if personal information was disclosed because of their unauthorised actions.

- **Education:**

- Staff and pupils are made aware of the risks and issues associated with communicating through e-mail and have strategies to deal with inappropriate e-mails. This is part of the school's e-Safety and anti-bullying education programme.