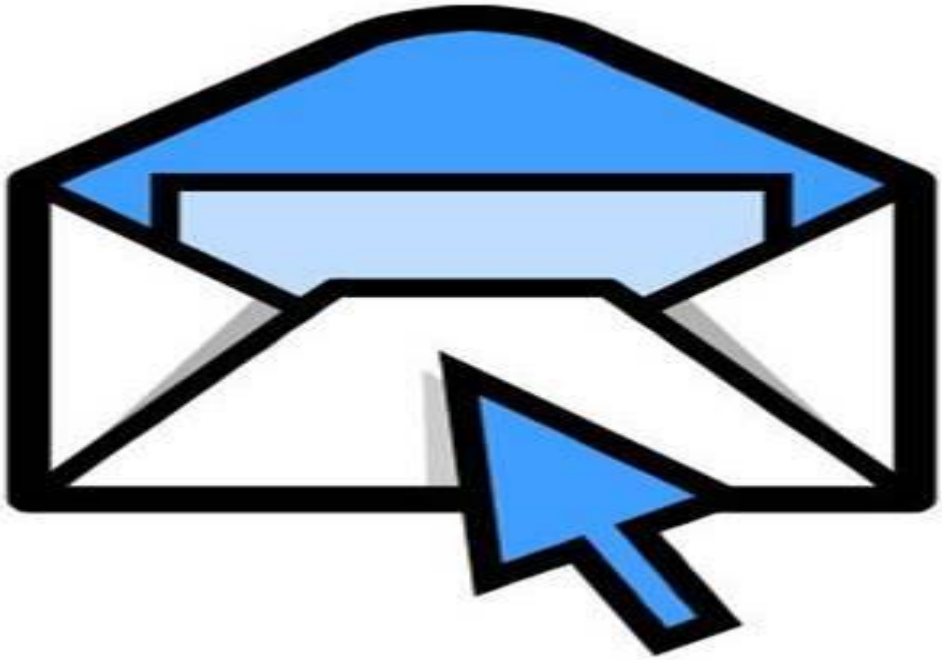
MAYVILLE PRIMARY SCHOOL



Policy: managing e-mail

Policy review Date: September 2016

How will e-mail be managed?

E-mail is now an essential means of communication for staff in our schools and increasingly for pupils and homes. Directed use of regulated e-mail in schools can bring significant educational benefits, increasing the ease of communication within Mayville Primary School community and facilitating 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.

Policy statements:

Mayville Primary School's Policy:

- We do not publish personal e-mail addresses of pupils or staff on Mayville Primary School website. We use post holder or group e-mail addresses, for example info@schoolname.la.sch.uk / head@schoolname.la.sch.uk / communication with the wider public.
- If one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law we contact the Police.
- Accounts are managed effectively, with up to date account details of users.
- Messages relating to or in support of illegal activities will be reported to the relevant Authority and Police.
- We use the Local Authority and additional email spam, phishing software provided by our LA / LGfL.
- Mayville Primary School prohibits any and material which may be related to extremism or radicalisation

Pupils:

- We use communication tools within the 'closed' Learning Platform (London MLE) with the pupils for communication with staff and other pupils. All this is audited.
- We do not use email that identifies the name and school of the pupil.
- We only use the LGfL London pupil email service.
- Pupils can only use the LGfL / school domain e-mail accounts on Mayville Primary School system.
- Pupils are introduced to, and use e-mail as part of the ICT scheme of work (KS2).
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and more generally (for example personal accounts set-up at home) i.e.
    - not to give out their e-mail address unless it is part of a school managed project or 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;
    - the sending of multiple or large attachments should be limited;

  - personal information should not be sent as attachments on open email. A secure method of encrypted transfer should always be used;
  - 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 of 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 Mayville Primary 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 use LA or LGfL e-mail systems for professional purposes.
- Staff are allowed to only use the LGfL / school domain e-mail accounts on Mayville Primary School system;
- We have a 'closed' LA secure email system which is used for some 'LA approved' transfers of information we consider to be sensitive (some protect-level data);
- We never use email to transfer staff or pupil level data. We use secure, LA / DCSF approved systems. These include: S2S (for school to school transfer); secure XML transfer of management information data transfer; *USO-FX (for LGfL user authentication);*
- We do not allow staff to access personal email during Mayville Primary School day;
- 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 Mayville Primary School 'house-style';
  - the sending of multiple or large attachments should be limited
  - personal information must not be sent as attachments on open email. A secure method of encrypted transfer should always be used.
  - the sending of chain letters is not permitted;
  - embedding adverts is not allowed;

- All staff sign our 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.

Further information on LGfL email services is available at www.email.lgfl.net

Becta email advice:
http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_com_02&rid=14906
Becta Information Handling Guidelines:
http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_mis_im03&rid=14734

DCSF advice on secure data transfer:
http://www.teachernet.gov.uk/management/ims/newsinfo/Bulletin/

Technology:

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 London have appropriate educational, filtered Internet-based e-mail options through the London Grid for Learning (LGfL).

- LondonMail – powered by Microsoft
- Safemail – a service providing restricted email is currently due to be launched across London in January 2010 subject to Microsoft releasing required safety enhancements.
- Visualmail – Powered by Fronter (aimed at primary)
- StaffMail – powered by Microsoft (operated by LGfL).

LondonMail is an email solution, which is filtered for inappropriate language and unsolicited mail, designed for pupil use in accordance with Becta Standards. It uses a common format for identity but at the same time appears anonymous. This means a pupil's school (and thus their age group, gender and location) are not identifiable. This conforms to Becta standards.

e.g. jbloggs031.301@lgflmail.net

Although this seems anonymous, because the account is linked to a LGfL sign-on database (USO) the account is always accountable and traceable.

Safemail is an email solution which will offer further restrictions on who the email can be sent to or received from. The aim will be to provide functionality that will restrict the email use to a selected level of Class, School or LA. (Please note: this is to provide an alternative to the existing Digital Brain safemail currently used by many schools as the current contract with Digital Brain VLE is ending in July 2010)

Visualmail is a feature of the London MLE and is an internal mail restricted to your school's MLE environment. Additionally the London MLE provides a variety of alternative options for communications within a closed network other than email.

Spam, phishing and virus attachments are all potential risks to be considered. Filtering software must be used to stop unsuitable mail. LGfL's filtering provision is highly efficient in this respect.

StaffMail is available to staff and governors within LGfL connected schools and LAs. It has the full functionality of a Microsoft Exchange account. It is only accessible where the LA has Unified Sign On (USO) in place. The service is suitable for those LAs that do not have a LA Corporate email system.

If you have a serious child protection issue using email you should refer this to your LA, (e.g. a child's disappearance may require investigative access).

Procedures:

In Mayville Primary 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, such as Hotmail, must be avoided by all working in schools and staff should be required to use appropriate LA or LGfL systems for professional purposes.

Individual pupil e-mails such as jbrown026.302@lgflmail.net which allow pupils to send and receive messages to and from the wider world, still need to be carefully allocated to appropriate situations. A school may not even need to use email anymore as communication can be achieved within the Learning Platform.

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. External web-based e-mail accounts with anonymous names such as pjb354@emailhost.com make monitoring and tracing very difficult and require support from the providers of the email system (who may be an international company).

Email must not be used by staff to transfer information about pupils – unless it is within an encrypted, secured email system, so you need to check with your Local Authority what their procedures are. 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.
[Email practice thus has relevance to your school Information Handling / security policy and should be consider both by Mayville Primary School's Senior Information Risk Officer (SIRO) and the Information Asset Owner should be named. Please see link to the Becta site on Information Handling Guidelines below.].

Education:

Staff and pupils need to be made aware of the risks and issues associated with communicating through e-mail and to have strategies to deal with inappropriate e-mails. This should be part of Mayville Primary School's e-Safety and anti-bullying education programme.

In addition to the Visualmail feature in the LMLE, there are programs that can be used with the youngest pupils that 'simulate' an E-mail system. This provides a useful environment to teach the skills of sending and receiving an e-mail with or without an attachment to very young pupils.

Pupils need to understand good ‘netiquette’ style of writing, (this links to English) and appropriate e-mail behaviour.
[Please note: to achieve a level 4 or above in ICT, pupils must have experienced sending and receiving e-mails.]