Spam (or Junk) email

- Always be vigilant when receiving or responding to emails.
- Make sure your spam filter is always switched on to minimise the risks.

The vast majority of email sent every day is unsolicited junk mail. Examples include:

- Advertising, for example online pharmacies, pornography, dating, gambling.
- Get rich quick and work from home schemes.
- Hoax blackmail messages
- Hoax orders
- Hoax virus warnings.
- Hoax charity appeals.
- Chain emails which encourage you to forward them to multiple contacts (often to bring 'good luck').

How spammers obtain your email address

- Using automated software to generate addresses.
- Enticing people to enter their details on fraudulent websites.
- Hacking into legitimate websites to gather users' details.
- Buying email lists from other spammers.
- Inviting people to click through to fraudulent websites posing as spam email cancellation services.
- From names/addresses in the cc line, or in the body of emails which have been forwarded and the previous participants have not been deleted.

The very act of replying to a spam email confirms to spammers that your email address exists.

How to spot spam

Spam emails may feature some of the following warning signs:

- You don't know the sender.
- Contains misspellings (for example 'p0rn' with a zero) designed to fool spam filters.
- Makes an offer that seems too good to be true.
- The subject line and contents do not match.
- Contains an urgent offer end date (for example "Buy now and get 50% off").
- Contains a request to forward an email to multiple people, and may offer money for doing so.
- Contains a virus warning.
- Contains attachments, which could include .exe files.

The risks

- It can contain viruses and spyware.
- It can be a vehicle for online fraud, such as phishing.
- Unwanted email can contain offensive images.
- Manual filtering and deleting is very time-consuming.

- It takes up space in your inbox.

Email Scams

Scams are generally delivered in the form of a spam email (but remember, not all spam emails contain scams). Scams are designed to trick you into disclosing information that will lead to defrauding you or stealing your identity.

Examples of email scams include:

- Emails offering financial, physical or emotional benefits, which are in reality linked to a wide variety of frauds.
- These include emails posing as being from 'trusted' sources such as your bank, HMRC or anywhere else that you have an online account. They ask you to click on a link and then disclose personal information.

Phishing emails

Phishing is a scam where criminals typically send emails to thousands of people. These emails pretend to come from banks, credit card companies, online shops and auction sites as well as other trusted organisations. They usually try to trick you into going to the site, for example to update your password to avoid your account being suspended. The embedded link in the email itself goes to a website that looks exactly like the real thing but is actually a fake designed to trick victims into entering personal information.

- The email itself can also look as if it comes from a genuine source. Fake emails sometimes display some of the following characteristics, but as fraudsters become smarter and use new technology, the emails may have none of these characteristics. They may even contain your name and address.
    - The sender's email address may be different from the trusted organisation's website address.
    - The email may be sent from a completely different address or a free webmail address.
    - The email may not use your proper name, but a non-specific greeting such as "Dear customer."
    - A sense of urgency; for example the threat that unless you act immediately your account may be closed.
    - A prominent website link. These can be forged or seem very similar to the proper address, but even a single character's difference means a different website.
    - A request for personal information such as username, password or bank details.
    - You weren't expecting to get an email from the organisation that appears to have sent it.
    - The entire text of the email may be contained within an image rather than the usual text format. The image contains an embedded link to a bogus site

Use email safely

- Do not open emails which you suspect as being scams.

- Do not forward emails which you suspect as being scams.
- Do not open attachments from unknown sources.
- **If in doubt, contact the person or organisation the email claims to have been sent by ... better safe than sorry.**
- Do not readily click on links in emails from unknown sources. Instead, roll your mouse pointer over the link to reveal its true destination, displayed in the bottom left corner of your screen. Beware if this is different from what is displayed in the text of the link from the email.
- Do not use links in emails to log into websites. Go to the Internet browser and type in the URL (web address) and log in manually from there.
- Do not respond to emails from unknown sources.
- Do not make purchases or charity donations in response to spam email.
- Don't click on 'remove from subscription' or reply to unwanted email.
- Check Junk mail folder regularly in case a legitimate email gets through by mistake.
- When sending emails to multiple recipients, list their addresses in the 'BCC' (blind copy) box instead of in the 'To' box. In this way, no recipient will see the names of the others, and if their addresses fall into the wrong hands there will be less chance of you or anybody else receiving phishing or spam emails.
- Similarly, delete all addresses of previous parties in the email string, before forwarding or replying.
- Most Microsoft and other email clients come with spam filtering as standard. To mark email as spam in Office 365 simply right click the message and select "Mark as Junk". For multiple messages select each via the tick box to the left of the message and click "Junk" at the top of the webpage.
- Junk emails are kept within the Junk folder for 30 days, marking as Junk helps the email filter to be aware of such messages.
- Most spam and junk filters can be set to allow email to be received from trusted sources, and blocked from untrusted sources.
- When choosing a webmail account such as Gmail, Hotmail and Yahoo! Mail, make sure you select one that includes spam filtering and that it remains switched on.
- If you are suspicious of an email, you can check if it is on a list of known spam and scam emails that some internet security vendors such as McAfee and Symantec feature on their websites. Or forward to the IT department

  helpdesk@newmillsschool.co.uk