3.5 If given access to the School email system or to the internet, staff are responsible for the security of their terminals. Staff are required to log off/lock screen when they are leaving the terminal unattended or when leaving the office to prevent unauthorised users accessing the system in their absence. The Senior Leadership Team may perform spot checks from time to time to ensure compliance with this requirement.

3.6 Staff should be aware that if they fail to log off/lock screen and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the Trust's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

3.7 Logging off/locking screen prevents another member of staff accessing the system in the user's absence and may help demonstrate in the event of a data breach that he or she was not the party responsible.

3.8 Staff without authorisation should only be allowed to use terminals under supervision. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with.

3.9 Members of staff who have been issued with a laptop or tablet must ensure that it is kept secure at all times, especially when travelling (e.g. stored safely in boot of car). Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event that the machine is lost or stolen. Staff should also observe basic safety rules when using such equipment e.g. ensuring that they do not use or display such equipment in isolated or dangerous areas. Staff should also be fully aware that if using equipment on public transport, documents can be easily read by other passengers.

4. Systems use and data security

4.1 Members of staff should not delete, destroy or modify any of the Trust's existing systems, programs, information or data which could have the effect of harming or exposing to risk or harm the School, its staff, pupils, or any other party. 8871 0 595.32 841.92 reW*nBT

- audio and video streaming (unless used for educational purposes from a reputable website);
- instant messaging;
- chat rooms;
- social networking sites; and
- personal email (such as Hotmail or Gmail).

4.5 No device or equipment should be attached to our systems without the prior approval of the IT department. This includes, but is not limited to, any telephone, USB device, digital camera, MP3 player, infra-red, Bluetooth connection device or any other device.

4.6 The Trust monitors all emails passing through its systems for viruses. Staff should be cautious when opening emails from unknown external sources or where for any reason an email appears suspicious (such as ending in .exe' or '.pdf' or clicking on any links which ask to re-enter your password or look suspicious). The IT department should be informed immediately if a suspected virus is received. The School reserves the right to block access to attachments to email for the purpose of effective use of the system and compliance with this policy. The Trust also reserves the right not to transmit any email message.

4.7 Staff should not attempt to gain access to restricted areas of the network or to any password-protected information unless they are specifically authorised to do so.

4.8 Misuse of the Trust's computer systems may result in disciplinary action up to and including summary dismissal. For further guidance on what constitutes misuse please see the section entitled "Inappropriate Use of the School's Systems" and guidance under "Email etiquette and content" below.

5. Email etiquette and content

5.1 Email is a vital business tool, but often lapses inappropriately into an informal means of communication and should therefore be used with care and discipline.

5.2 The Trust's email facility is intended to promote effective communication within the Trust on matters relating to trust and its' school's activities and access to the Trust's email facility is provided for work purposes only.

5.3 Staff are permitted to make reasonable personal use of the Trust's email facility provided such use is in strict accordance with this policy (see "Personal Use" below). Personal subscriptions using the Trust email facility may open the system to phishing and it is the responsibility of all staff to protect the system by minimising personal use. Excessive or inappropriate personal use of the Trust's email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary dismissal depending on the seriousness of the offence.

5.4 Staff should always consider if email is the appropriate medium for a particular communication. The Trust encourages all members of staff to make direct contact with

6. Use of the web and the internet

6.1 When a website is visited, devices such as cookies, tags or web beacons may be deployed to enable the site owner to identify and monitor visitors. If the website is an inappropriate one such a marker could be a source of embarrassment to the Trust. Staff may even be committing a criminal offence if, for example, the material is pornographic in nature.

6.2 Staff must not therefore access from the Trust's system any web page or any files (whether documents, images or other) downloaded from the web which, on the broadest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK it may be in sufficient bad taste to fall within this prohibition.

6.3 As a general rule, if any person within the Trust (whether intending to view the page or not) might be offended by the contents of a page, or if the fact that the Trust's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy. rust (whether intending to 16.62 Tm0 g0 G[(wh)-6

- forwarding electronic chain letters and other materials;
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

8.3 Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

8.4 Where evidence of misuse is found the Trust may undertake a more detailed investigation in accordance with our Disciplinary Policy and Procedure, involving the examination and disclosure of documents, systems and monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

8.5 If necessary, such information may be handed to the police in connection with a criminal investigation.

9. Taking information offsite

9.1 The Trust allows staff to take children's workbooks off site for the purposes of marking and assessment. These should be treated in the same way as laptops and tablets in that reasonable measures both at home and in transit should be made to keep them safe.

9.2 When taking pupils off site for educational visits, it is standard practice to take a hard copy of pupil contact details and health care plans etc. in case of emergency. Owing to the sensitivity of this kind of information, a greater degree of care should be taken to keep the information secure and confidential. For the avoidance of doubt, such information must never be left unattended (unless it is securely locked away) or left in a place where it can be accessed by others. Wherever possible, information should be kept in a lockable bag. On return, the hard copies must be handed back into the school office who will shred them.

9.3 There will be occasions when highly sensitive meetings cannot take place within the Trust or school building e.g. child protection conferences and strategy meetings. In these instances, it may be necessary to print off hard copies of highly confidential information for the purposes of the meeting. Only designated personnel (the Principal, SENCO and Pastoral Manager) have the automatic right to do this. Information taken off site must be logged and signed off and shredded on return to site. The same steps as documented in 9.2 should be taken to safeguard the information.

9.4