The Tiffin Girls' School

E-SAFETY POLICY

ADOPTED JULY 2015

Introduction

1. The use of ICT resources is now a key aspect of our day-to-day work and social interaction. It is important that the school has a robust E-Safety policy in place that helps to manage our stakeholders' use of ICT resources and supports safe and appropriate engagement with them.

2. This document should be read in conjunction with:
   - Staff Code of Conduct
   - Data Protection Policy
   - Behaviour for Learning Policy
   - Safeguarding Policy
   - Freedom of Information Publication Scheme

3. This document incorporates, and therefore supercedes the ICT Acceptable Use Agreement and the Web Filtering Policy

4. The Tiffin Girls' School E-Safety Policy is an umbrella term for a series of four documents:
   - Staff Professional Identity (page 3)
   - Secure Data Handling (page 8)
   - Use of the Network by Students (page 14)
   - Use of the Network by Staff (page 21)

5. Together these documents intend to support the school's management of our internal network and ICT resources whilst supporting positive e-safety behaviours which are developed for staff, students and parents via:
   - Staff Training
   - Parent Focus Evenings delivered by expert speakers
   - Student engagement with the pastoral programme, via school council
   - A dedicated E-Safety page on the school's main website (under both the *Parent* and *Student* tabs)

6. As a school, we are very aware of the importance of guiding young people in their use of new media and technology. We are committed to ensuring that we share information and good practice on how to manage safe use of the internet and technology with all stakeholders.

7. Typically around 20% of a young person's engagement with online media occurs in school and so within a managed network environment. This means that a significant aspect of our E-Safety Policy must recognise the school's role in shaping behaviours that dictate students' use of the internet outside of school.

Monitoring and Review

8. The policy will be monitored and evaluated regularly taking into account any incidents which occur, technological developments which might need a change in the policy or changes in legislation.

DOCUMENT 1: STAFF PROFESSIONAL IDENTITY

9. The need for everyone to use electronic communications grows apace. The school provides guidance on how staff can protect themselves from potential harassment when using electronic communications, and on how to protect the identity and image of The Tiffin Girls' School.

Definitions

10. Electronic communications equipment includes (but may not be limited to):
    - Telephones, faxes, voice-mail, computers, laptops, internet, mobile phones (all types, including smart phones), tablets, photocopiers, digital cameras, walkie-talkies, web cameras, videos and palm-held equipment.

11. Types of communication can include (but may not be limited to):
    - Telephone calls, email, text messaging, multimedia messaging ,transmission of photographs and moving pictures, contact via websites and social network sites, blogging, wikis, contact via web cameras and internet phones.

Objectives

12. This policy aims to provide information and guidance to protect school staff from harassment, real or alleged, misuse, and any consequential disciplinary action arising from the misuse of electronic communication equipment in or outside school. It is also intended to ensure that the school's equipment is used responsibly and safely at all times.

Professional identity protection – summary:

13. In communications with pupils and parents, **never** give out personal information which identifies your:
    - Home address.
    - Telephone number.
    - Personal mobile phone number.
    - Personal email address.

14. Once such information is known, you are open to harassment through unwanted phone calls, text messages and emails.

Personal Identity Protection: Individual responsibility

On school business:

15. Make sure you do not allow people to see personal or confidential school information when a computer is left unattended. Log off, turn it off and set up a password-protected screen saver to prevent unauthorised access.

16. Keep all passwords and login details strictly private and always remember to log off correctly after using the computer. Never allow anyone else to use your personal login detail because you will then be held responsible for their on-line activity.

17. Always use the school's digital camera or video camera for taking pictures and upload them onto a school computer. Once uploaded, the images should be deleted from the camera's memory. Photographs of pupils should not be taken home to use on a personal computer.

18. Always speak professionally and respect confidentiality and be aware that the message could be overheard at either end when using any hand-held school walkie-talkies or any other hands-free devices.

19. If you are using school electronic equipment off-site, then take the same level of care as you would in school. A digital camera taken off-site should not be returned to school with personal photographs on it.

20. Do not make personal financial transactions on any school equipment because information may become accessible to others.

21. All school business should be carried out using your work email address.

22. Never give a personal email address to pupils/parents

23. It is impossible to control what information is sent to a member of staff by email. However if offensive, obscene and/or discriminatory material is received, the recipient must report it immediately, and in writing, to the Deputy Head (Infrastructure) or the Headteacher. Never send a reply. Keep a printed copy of the email as evidence and pass a copy of the email to the Deputy Head or Headteacher. Ensure that the sender's information is also recorded because their email service provider may take action.

24. Observe sensible precautions when taking photographs which may include pupils. Make sure that individual pupils cannot be identified by name, especially if the photograph is for use on the school website or MLE.

Using social media

25. Staff should not use school facilities to access or update their personal social networks.

26. Ensure you do not:
    - Accept pupils and/or parents as 'friends' on your personal social network site.
    - Use your school email address as contact on any social networking sites.
    - Add photos from school events or trips which include photos of pupils.

27. Ensure you:
    - Consider carefully your use of chat rooms, instant messaging or other social networking services which may be accessed socially by pupils and are not monitored by the school.
    - Protect your social network site by using the correct up-to-date privacy settings.
    - Make sure that personal information cannot be seen from the links to your friends' sites.
    - Keep the content of any personal blogs of an acceptable professional standard because any inappropriate use has the potential to be misinterpreted and could bring the school into disrepute.
    - Attach a disclaimer to any personal blogs that the views expressed are personal and not necessarily those of the school.

28. Photographs and descriptions of activities in the personal life of staff may also not be considered appropriate if viewed by other staff, pupils or parents.

- Staff should be aware that, even if they have used the privacy settings, they may not be able to prevent material becoming public from their 'friends' sites.
- It is recognised that these on-line communications tools, such as weblogs ('blogs') and wikis, have a potentially useful role in schools – such as on school websites, learning journals, celebrating good work, sharing information and facilitating collaboration. Where pupils and their families are sharing these tools with staff in school it is important that this should always be through a school-based provision, such as the school learning platform/MLE, using a school log-in where all communication is open and transparent.

Action you must take if you discover inappropriate (threatening or malicious) material on-line concerning yourself or your school

29. Both the school and members of staff are vulnerable to material being posted about them on-line. All staff should be aware of the need to report this should they become aware of anything bringing the school or colleagues into disrepute.

30. Secure and preserve any evidence. For example, note the web address (URL) or take a screen shot or copy and print the screen. Report it immediately to your line manager or Headteacher.

31. All social network sites have the means to report unacceptable material or activity on their site – some more readily available than others. If the material has been created by a pupil or parent, then the school has a responsibility to deal with it. The school will contact the uploader of the material or the internet service provider/site administrator and ask for the material to be removed.

Professional identity protection – the school's responsibility

32. The school will:
    - Enforce the Behaviour for Learning Policy to protect staff and pupils from malicious use of mobile phones, in particular the use of camera and video-phones.
    - Ensure that the policy and procedures for home-school communication are shared with, and understood by, all staff.
    - Establish whole school systems for dealing with inappropriate communications and breaches of security.
    - Provide all staff with an individual email address to be used for all school-related communications by every member of staff.
    - Enforce the policy for monitoring the use of the school's electronic equipment by staff, including procedures for accessing email and files when staff are absent. Appropriate checks with the owner will be made before any action is undertaken.
    - Provide digital cameras and mobile phones which can be borrowed by staff as required for all school-related work, including trips. These mobile phone numbers should be used on the emergency parental telephone trees for trips.
    - Provide a safe learning environment, such as a MLE, for electronic communications with pupils.
    - Ensure there are established systems for reporting unwanted or accidental electronic communications and that all staff are aware of the correct person to report any issues to.
    - Ensure all incidents reported are correctly recorded and that such incidents are always treated seriously.
    - Create procedures to regularly check the school's presence on the web to ensure material detrimental to the school is not published.

Real time on-line communication

33. The ability to communicate in real time using the computer and other electronic devices (such as mobile phones) makes these an excellent tool for a range of educational purposes. However, staff should take the same level of care with these tools as they would if working in a face-to-face situation with a pupil or group of pupils.

34. Access should always be through a school created account, never a personal account, and it should be focused on a clearly specified educational objective.

35. There are likely to be times when this kind of activity will happen outside normal school hours and perhaps off the school premises e.g. visits, fixtures, field trips etc. In this situation, it should always be carried out with the full knowledge and agreement of your line manager or Headteacher.

36. Staff should be aware that they must remain focused on the educational purpose of the communication and never allow it to become a social occasion.

37. When a web camera is used it should have a clear purpose. Staff should be aware of the ability of meetings of this kind to be recorded without their knowledge. However, they may wish to use this function for their own security, as long as all parties are informed that recording is taking place.

38. Staff must protect their privacy by never allowing pupils or parents to obtain their mobile phone number or leave their mobile phone where it could be accessed by a pupil.

39. Action staff **must** take if an incident occurs:
    - Report immediately, and in writing, to your line manager or Headteacher.
    - Do not reply to abusive or worrying text or video messages.
    - Do not delete messages. Keep them for evidence.
    - Use 1471 to try and obtain the number if you can. Most calls can be traced.
    - Report it to your phone provider and/or request a change of number.
    - Technical staff may also be able to help you to find or preserve evidence e.g. logs of the call.

40. Employees must not use school equipment (including their school provided laptop) to:
    - Store, view, download or distribute material that is obscene, offensive or pornographic, contains violent images, or incites criminal behaviour or racial hatred.
    - Store, view, download or distribute material that may breach intellectual property rights (e.g. use of copyrighted images or logos)
    - Gamble.
    - Undertake political lobbying.
    - Promote or run a commercial business.
    - Download or distribute games, music or pictures from the internet for personal use. They can bring viruses with them, use up capacity on the servers and potentially breach copyright.
    - Send emails, texts or messages or publish anything on a website, social networking site or blog, which:
        - Is critical about members of the school community, including pupils.
        - Are likely to be misinterpreted by the recipient in terms of tone or manner.
        - Contain inappropriate comments which could cause offence or harassment on the grounds of gender, race, disability, age, religion or sexual identity.

    - Has originated from a chain letter.
- Conduct private and intimate relationships via email.
- Spend school time on personal matters (e.g. arranging a holiday, shopping, looking at personal interest websites). This may be treated as misconduct.
- Store personal information on the school network (e.g. personal photos, screensavers or wallpaper).
- Download or copy software (excluding software updates).
- Use the email system to transmit any documents or software without checking the copyright or licence agreement.
- Install software licensed to the school on a personal computer unless permission to do so is explicitly covered by the school licence agreement.
- Take, transmit or publish pictures of a member of staff or pupil on your mobile phone, camcorder or camera without the person's permission.
- Give away email lists for non-school business.

Monitoring and privacy

41. The school's email and internet facilities are business systems, owned by the school. The school therefore reserves the right to monitor all use of the internet and of the school's ICT systems in line with guidance. Usage will be monitored to ensure that the systems are being employed primarily for business and educational reasons, that there is no harassment or defamation taking place and that employees are not entering into illegal transactions.

42. Staff need to be aware that internet sites visited are traceable, and that deleted or trashed messages or attachments can be recovered.

43. Email, telephone calls and internal and external post (unless clearly identified as private and confidential post) should be used primarily for business and educational purposes.

44. School managers have proxy access to all the school's communication systems for monitoring and interception of communications in order to deal with matters in an employee's absence for holiday, illness or other reason.

45. Any material stored on the school's network or being circulated via the school's email system has no rights of individual privacy. In accordance with RIPA (Regulation of Investigatory Powers Act 2000) monitoring or surveillance without an employee's knowledge can be carried out on internal email systems or information stored on a server.

Breaches of this policy

46. Breach of this policy could lead to disciplinary action against you in accordance with the school's disciplinary policy.

47. Where breaches involve third parties, including pupils, parents or other individuals, the police will be involved as appropriate and the Crown Prosecution Service (CPS) Guidelines (20 June 2013) regarding prosecuting cases involving communications sent via social media will be used.

DOCUMENT 2: SECURE DATA HANDLING

48. Legislation which applies is The Data Protection Act 1998. Other useful documents include:
    - Information Sharing: Guidance for Practitioners and Managers HM Govt. Oct 2008 and
    - Information Commissioner's Office (ICO) – *'What is personal Data –quick reference guide'* *http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/determining_what_is_personal_data_quick_reference_guide.ashx*

Background

49. Schools need to ensure the safety and security of any material of a personal or sensitive nature. Legislation covering the safe handling of this data is addressed by the UK Data Protection Act 1998 and, following a number of losses of sensitive data, a report was published by the Cabinet Office in June 2008 regarding Data Handling Procedures in Government. This stipulates the procedures that all departmental and public bodies should follow in order to maintain security of data and which the school has adopted through this policy and practice.

Introduction

50. This secure data handling policy applies to all forms of personal data, regardless of whether it is held on paper or in electronic format. It is the responsibility of all members of the school community to take care when handling, using or transferring personal data so that it cannot be accessed by anyone who does not:
    - Have permission to access that data
    - Need to have access to that data

51. Any loss of personal data can have serious effects for individuals and/or the school. It can bring the school into disrepute and may well result in disciplinary action and/or criminal prosecution for individuals. All transfer of data is subject to risk of loss or contamination.

52. Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in current relevant data legislation and regulations. It is important that the school has a clear and well understood personal data policy because:
    - No school or individual would want to be the cause of any loss of personal data, particularly as the impact of data loss on individuals can be severe and cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation
    - Schools are 'data rich' and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
    - The school will want to avoid the criticism and negative publicity that could be generated by any loss of personal data
    - The school is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation

53. Schools have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in school but also from remote locations.

54. The school and individuals working in the school will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This can include:
    - Personal information about members of the school community – including pupils/students, members of staff, parents and carers e.g. names, addresses, contact details, legal guardianship, health records, disciplinary records
    - Curricular/academic data e.g. class lists, pupil/student progress records, reports, references
    - Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
    - Information that might be disclosed by parents/carers or by other agencies working with families or staff members

Principles

55. As the role of management information systems (MIS) continues to develop, staff in schools have increasing access to a wide range of sensitive information. There are generally two types of sensitive information including (but not limited to):
    - Personal data concerning the staff and pupils
    - Commercially sensitive financial data

56. It is important to ensure that both types of information are managed in a secure way at all times. Personal data is the most likely form of sensitive data that a school will hold. Personal data is defined by the Data Protection Act *as 'Data relating to a living individual who can be identified from the data'*. The Act gives eight principles to bear in mind when dealing with such information. Data must:
    - Be processed fairly and lawfully
    - Be collected for a specified purpose and not used for anything incompatible with that purpose
    - Be adequate, relevant and not excessive
    - Be accurate and up-to-date
    - Be processed in accordance with the rights of the data subject
    - Be kept securely
    - Not be kept longer than necessary
    - Not be transferred outside the EEA (European Economic Area) unless the country offers adequate protection

57. The Data Protection Act states that some types of personal information demand an even higher level of protection. This includes information relating to:
    - Racial or ethnic origin
    - Political opinions
    - Religious beliefs or other beliefs of a similar nature
    - Trade union membership
    - Physical or mental health or condition
    - Sexual life (identity)
    - The commission or alleged commission by them of any offence, or any proceedings for such or the sentence of any court in such proceedings

58. The three questions below can be used to quickly assess whether information needs to treated securely:
    - Would disclosure/loss place anyone at risk?

- Would disclosure/loss cause embarrassment to an individual or the school?
- Would disclosure/loss have legal or financial implications?

59. If the answer to any of the above is 'yes', then it will contain personal or commercially sensitive information and needs a level of protection.

Purpose

60. The purpose of this policy is to advise all members of staff what is required by The Tiffin Girls' School to ensure that the school complies with the Data Protection Act at all times and to advise all members of staff how to handle data securely.

Procedures and practice

61. The following practices will be applied within The Tiffin Girls' School:
    - The amount of data held by the school will be reduced to a minimum
    - Data held by the school must be routinely assessed to consider whether it still needs to be kept or not
    - Personal data held by the school will be securely stored and sent by secure means

Auditing

62. The school must be aware of *all* the sensitive data it holds, be it electronic or paper. Therefore:
    - A list (Appendix 1) will be kept detailing the types of sensitive data held, where and by whom, and will be added to as and when new data is generated.

Risk assessment

63. The school's risk assessment will generally involve answering the following questions:
    - How sensitive is the data?
    - What is the likelihood of it falling into the wrong hands?
    - What would be the impact of the above?
    - Does anything further need to be done to reduce the likelihood?

64. After assessing risk, the school will decide how to reduce any risks or whether they are at an acceptable level.

65. Appendix 2 provides a staff help sheet for assessing the risk of sharing information.

66. Risk assessment will be an on-going process and the school will carry out assessments at regular intervals because risks change over time.

Securing and handling data held by the school

67. The school will encrypt any data that is determined to be personal or commercially sensitive in nature. This includes data held on fixed station computers, laptops, portable devices and memory sticks.

68. All staff will be trained to understand the need to handle data securely and the responsibilities incumbent on them.

69. Staff should *not* copy or remove sensitive data from the school or authorised premises unless the media are:

- Encrypted
- Transported securely
- Stored in a secure location

70. Sensitive data *should not* be transmitted in unsecured emails (e.g. pupil names and addresses, performance reviews etc.)

71. Data transfer should be through secure websites. If this is not available, then the file must be minimally password protected or preferably encrypted before sending via email. The password must be sent by other means, and on no account included in the same email. A record of the email should be kept to identify when, and to whom, the email was sent. (The DFE website contains a useful section – '*Transferring personal data securely between schools, LAs and the Department*' (updated April 2012). This provides comprehensive guidance on transferring information.)
http://media.education.gov.uk/assets/files/pdf/s/secure%20methods%20for%20transferring%20data.pdf

72. Data (pupil records, SEN data, contact details, assessment information) must be automatically backed up, encrypted and stored in a secure place, e.g. safe/fire safe/remote backup facility.

73. All staff computers, including laptops, must be used in accordance with the policies use of the internet and intranet by staff and pupils.

74. When laptops are passed on or re-issued, data will be securely wiped from any hard drive before the next person uses it (not simply deleted). This will be done by the school's ICT technical support staff.

75. The school's wireless network (Wi-Fi) will be secure at all times.

76. The school will identify which members of staff are responsible for data protection.

77. The school will ensure that staff who are responsible for sets of information, such as SEN, medical, vulnerable learners, management data etc. know what data is held, who has access to it, how it is retained and disposed of. Appendix 1 details which members of staff are responsible for which data.

78. Where a member of staff has access to data remotely, the remote access off the school site to any personal data should be over an encrypted connection (e.g. VPN) protected by a username/ID and password. *This MIS information/school data must not be stored on a personal (home) computer.*

79. Members of staff who are given full, unrestricted access to the school's management information system must access the systems over an encrypted connection. *This MIS information/school data must not be stored on a personal (home) computer.*

80. The school will securely delete commercially sensitive or personal data when it is no longer required according to the Records Management Society's guidance.

APPENDIX 1

Sensitive Data	Where held	By whom
Single Central Record	Network	Leadership Support and Cover Co-ordinator
Safeguarding Records	Network / secure paper files	Designated Teacher
SIMS data	Network	By all staff depending on levels of permission
Student Records (paper) including, but not limited to medical information, SEN, Pupil Reports, Letters to Parents, Class based assessments, exam results, whole school data	Network / secure paper files	All members of staff as appropriate and with set levels of permission
Trip Information	Network / secure paper files	Assistant Headteacher, Trip co-ordinators, Finance
Personnel Records	Network / secure paper files	Headteacher, HR Director, Leadership Support and Cover Co-ordinator depending on levels of permission
Performance Management records	Network / BlueSky / secure paper files	Headteacher, HR Director, Deputy Headteacher and line managers as appropriate with set levels of permission

APPENDIX 2

Staff help sheet for assessing risk of sharing information

In deciding the most appropriate way to share information and the level of security required, always take into consideration the nature of the information and the urgency of the situation, that is, take a risk-based approach to determining appropriate measures. The simplified process described below will help members of staff and the school itself choose the appropriate level of security needed when sharing potentially sensitive information.

Step 1

Imagine a potential security breach (e.g. a confidential letter is left in a public area, a memory stick is lost or someone reads information on a computer screen while waiting to meet a member of staff), and consider:

- Will it affect or identify any member of the school or community?
- Will someone lose/be out of pocket by more than £100?
- Will it cause any kind of criminal case to fail?
- Is there a risk of discomfort/slur upon professional character of someone?
- Is anyone's personal safety at risk?
- Will it embarrass anyone?

If the answer to all the above questions is 'no', the document does not contain sensitive information. If the answer is 'yes' to any of the questions above then the document will include some sensitive information and therefore requires a level of protection.

Step 2

Imagine the same potential security breach as above, and consider:

- Will it affect many members of the school or local community and need extra resources locally to manage it?
- Will an individual or someone who does business with the school lose/be out of pocket by £1,000 to £10,000?
- Will a serious criminal case or prosecution fail?
- Is someone's personal safety at a moderate risk?
- Will someone lose his or her professional reputation?
- Will a company or organisation that works with the school lose £100,000 to £1,000,000?

If the answer to any of the above questions is 'yes' then the document contains sensitive information and additional security should be considered such as password protecting the document before you email it to a colleague outside of the school. However, if you think that the potential impact exceeds that stated in the question (e.g. someone's personal safety is at high risk) think very carefully before you release this information at all.

Step 3

All documents that do not fit into steps 1 or 2 might require a higher level of protection/security if released at all. Err on the side of caution and seek guidance from the relevant line manager/senior member of staff.

DOCUMENT 3: USE OF THE NETWORK BY STUDENTS

Background

81. Information and Communications Technology (ICT) prepares pupils for a rapidly changing world in which many activities are transformed by access to a varied and constantly changing and developing technology.

82. ICT is a vital tool in the process of teaching and learning. Pupils use ICT tools to find and process information. This needs to be done responsibly, creatively and with discrimination. Pupils learn how to employ ICT to enable rapid access to ideas and experiences from a wide range of sources. All staff and pupils need to become confident users of ICT so that they can develop the skills, knowledge and understanding, which enables them to use appropriate ICT resources effectively as powerful tools for teaching and learning.

83. The internet provides children and young people with a wealth of opportunities for their entertainment, communication and education. But there are also risks of harm through the deliberate behaviour of others online, and through exposure to inappropriate content.

84. The Tiffin Girls' School has procedures in place to safeguard all learners from unlawful, sexual or otherwise potentially harmful content on the internet. Information on internet safety and the importance of monitoring internet use training at home is provided by the school regularly.

85. **At The Tiffin Girls' School ALL OUR SYSTEMS ARE CLOSELY MONITORED**

Introduction

86. This section of the E-Safety Policy is in place for use of these ICT facilities by pupils. There is a separate section of the policy for use by staff.

87. There are many computers available for use by pupils and the majority of these have access to the internet through the school network. All pupils have a login name, password and an email account. The email system is available for use both from within the school and externally using a web browser. There are specialist centres serving design, mathematics and science departments together with general purpose rooms. A growing number of other computers are located within individual departments/classroom areas and this will be supported by students increasingly using their personal devices on our network.

88. The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:
    - Pupils can only access data to which they have right of access
    - No pupil should be able to access another's files without permission
    - Access to personal data is securely controlled in line with the school's personal data policy
    - All network services are monitored and filtered
    - Logs are maintained of access by pupils and of their actions while users of the system
    - Students are provided with strategies to support their safe and appropriate use of ICT resources via the Pastoral Programme. This training underpins our E-Safety framework and allows for the network to be managed rather than locked down

Action plan

89. The following code of practice must be adhered to by all pupils. All pupils are expected to sign the ICT: Pupil acceptable usage agreement (see appendix 3) and all visiting pupils are expected to sign the ICT: Visiting pupils acceptable usage agreement (see appendix 4).

Rights of access – pupils

90. A safe and secure username/password system is essential and will apply to all school ICT systems, including email, Office 365 and Managed learning environment (MLE).

91. All passwords are generated by the network manager/ICT technical support staff and are unique to each pupil. Passwords can only be reset by the user or by the ICT technical team. All pupils will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the network manager and these will be reviewed, at least annually. The 'master/administrator' passwords for the school ICT system used by the network manager/ICT technical support team are also available to the Headteacher or other nominated senior leaders and kept in a secure place (e.g. school safe). In the event of a serious security incident, the police may request, and will be allowed access to, passwords used for encryption.

ICT code of practice for pupils

92. The facilities are provided to support and enhance curriculum-related activities. Each pupil will be issued with her own username and password, which must be kept confidential. Pupils must remember to log off when they have finished using the computer and/or software provided by the school anywhere. It is good practice to change passwords regularly.
    - The pupil's school email address must always be used for all school-related activity. Personal emails must not be used for any school-based activity.
    - The use of another person's user name and password, abusive language, sending abusive messages are all serious offences.
    - Students must not attempt to alter computer settings that are prohibited by network restrictions.
    - Pupils must not copy, alter, print or change another pupil's work in any shape or form without the person's prior knowledge and consent. Please note that copyright regulations apply to electronic publications as they do to paper.
    - Pupils must use the internet and printing facilities only to support their school work.
    - Pupils should be aware that information on the internet may not always be reliable and sources should be checked. Also websites are used for advertising material, which may influence the contents.

93. Emails are not confidential and do go astray. Therefore we must guard against any abuse which will bring the school into disrepute.
    - Pupils must not disclose to anyone on the internet their home address, telephone number, the name of the school or a photograph of themselves unless specific permission is given from a member of staff. Nor should they ever arrange to meet anyone unless this is part of a school project approved by their teacher.
    - Pupils must never pretend to be anything or anyone that they are not
    - Pupils must not engage with internet chatrooms in school

- If a pupil sees something which makes her feel worried or uncomfortable, she should report it immediately to a member of staff and never respond to bullying, suggestive or unpleasant emails or blog entries.
- Pupils must not send abusive email, chain email, excessive quantities or excessive sized emails. Nor must they use email to send or encourage material that is pornographic, illegal, offensive or invades another's privacy.
- Laptops, ipads, tablets and similar devices which are used on the school network fall under the same restrictions of use as networked computers.

Webfiltering

94. Requests for currently blocked sites to be made accessible on the school's network should be made to the ICT Services Manager via email which includes a link to the site requested and outlines the educational rationale for access to the website.

95. The ICT Services Manager will pass this onto a member of the Senior Leadership Team ('SLT') responsible for pastoral care.

96. The SLT member will evaluate the site and decide whether access should be allowed and will communicate this to the member of staff who made the request and the ICT Services Manager.

97. The SLT member will discuss with other members of SLT and seek expert advice if necessary.

98. The decision to allow access to a website can and will be reversed should it be deemed necessary by the SLT

Misuse of computer systems by pupils

99. Pupils must not vandalise the system by:
    - Physical damage.
    - Changing configuration or cabling unless specifically directed by a member of staff.
    - Hacking of the school or external systems.
    - Changing the contents of the hard disks.
    - Downloading or installing software onto the network, unless written as part of an approved school computer project and with the teacher's permission.
    - Bringing food and drink into computer areas or in the vicinity of classroom computers because spillages can cause serious damage to electronic equipment.

100. Serious offences and other inappropriate use of ICT facilities will result in the following sanctions:
    - An immediate ban from the network pending investigation.
    - A letter home informing parents of incorrect ICT use and a minimum ban of two weeks from the internet/email facilities.
    - Subsequent offences will lead to a four to eight week ban and/or an exclusion of up to three days from school.
    - More serious or long term abuse will lead to a total network ban and possible permanent exclusion from school.

101. Pupils found to be in contravention of this policy will be dealt with in line with the school's Behaviour for Learning Policy.

102. Using other pupils' accounts or accessing restricted file areas are considered to be serious offences. The network manager will record the offence and will immediately inform the Head of Year of the situation. Suspension of a pupil's access to all ICT facilities may take place after the Head of Year has informed the appropriate staff. The length of the ban may vary according to circumstances. To restore access, a note is required from the Head of Year / AHT Pastoral.

103. If a pupil damages hardware, the network manager will contact the main office staff. A letter will be sent to parents. The pupil will be charged for the damage.

104. Under exceptional circumstances, such as abuse which may be detrimental to the school network, the network manager may disable a pupil's account with immediate effect.

APPENDIX 3

ICT: Pupil acceptable computer usage agreement
Two copies should be signed - *one to be returned to school for the pupil file and the other retained by pupil/parents for reference.*

Guideline for all users of the school network
Access to the school network and internet is provided for you to carry out recognised schoolwork. This provision will only be made on the understanding that you agree to follow these guidelines. If you are being educated at another school or educational site, you are expected to follow these same guidelines.

We aim to support students' safe and appropriate use of the internet both in school and more broadly. This policy is designed to both set expectations (managing use) and support the behaviours that lead to students understanding their e-safety.

- Computer (file) storage areas are treated as school property. ICT staff may look at files and communications to ensure that the system is being used responsibly. I understand that I cannot expect my work and emails to be private
- I am aware that a member of staff could view my computer screen, from the school network, without my knowledge, at any time.
- I understand that I am responsible for good behaviour and that general school rules apply whilst using the computers.
- I understand that eating, drinking, personal grooming or the use of aerosol sprays near a computer may cause serious damage and are strictly prohibited.
- I will not reveal my password to anyone. If I think someone knows my password, then I will inform a member of the IT Technician team.
- I will not use another person's user id or password. If I am doing shared work I will ensure that I have my own saved version.
- I understand that programs must not be loaded or installed on a computer except by ICT support staff. I will not bring programs in on removable media, email or download them from the internet.
- I understand that the use of the internet is a privilege and provided for pupils to conduct genuine research and communicate with others.
- I understand that all the internet sites that I visit are recorded.
- I understand that I must not download any files without permission.
- I understand that I must not use instant messengers (e.g. AOL IM, Yahoo Pager, MSN) which are not provided by the School.
- I understand that I must not use web mail, other than that provided for my school account.

- I understand that I must not use obscene or offensive language. I will remember that communication should be polite to maintain the good reputation of the school.
- I understand that I must not seek out any offensive material.
- I understand that I must not complete mailing lists or subscription forms on the internet for personal use.
- I understand that I must not violate copyright laws. (Never copy and make use of any material without giving credit to the author. Copyright, Designs & Patents Act 1988). If I am unsure then I will ask a member of staff for advice.
- I will adhere to the E-safety policy: Use of the Network by Students

Sanctions

- I understand that violations of the above rules will result in action being taken following an investigation into the incident by an appropriate staff member.

The School reserves the right to seek remuneration from parents of pupils who cause malicious damage to ICT equipment.

During lessons, teachers will guide pupils toward appropriate materials. However, outside lessons, families bear this responsibility.

Please sign both copies - return one copy to the school and retain the second copy for your records.

We agree to the terms and conditions of the ICT: Pupil acceptable computer usage agreement.

Name of pupil: ……. Tutor group: ……..

Pupil's signature: …… Date: ……

Parent/Carer's signature: …… Date: ……..

APPENDIX 4

ICT: Visiting pupil acceptable computer usage agreement

As a visitor to The Tiffin Girls' School we ask you to act sensibly and properly at all times and accept the guidelines for visitors who use the school network. Access to the school network and internet is provided for you to carry out recognised schoolwork. This provision will only be made on the understanding that you agree to follow these guidelines.

- Computer (file) storage areas are treated as school property. ICT staff may look at files and communications to ensure that the system is being used responsibly. I do not expect my work and emails to be private
- I am aware that a member of the ICT staff could view my computer screen, from the school network, without my knowledge, at any time.
- I will not reveal my password to anyone. If I think someone knows my password, then I will change it.
- I will not use another person's user id or password. If I am doing shared work Ii will email a copy to my friend.
- I understand that programs must not be loaded or installed on a computer except by ICT support staff. I will not bring programs in on removable media, email or download them from the internet.
- I understand that all the internet sites that I visit are recorded.
- I understand that if I find inappropriate material I will advise the teacher immediately.
- I understand that I am always subjected to the Data Protection Act 1998, Computer Misuse Act 1990 and Copyright, Designs and Patents Act 1988.

Sanctions

- If you cannot act sensibly and properly your teacher will remove you from the computers and further action may be taken.

The School reserves the right to seek remuneration from parents of pupils who cause malicious damage to ICT equipment.

Please sign and return to your teacher

I agree to the terms and conditions of The Tiffin Girls' School's ICT: Visiting pupil acceptable computer usage agreement.

Name of pupil: ……. School: ……

Pupil's signature: …… Date: …….

DOCUMENT 4: USE OF THE NETWORK BY STAFF

Background

105. Information and Communications Technology (ICT) is a vital tool in the process of teaching and learning. Teachers prepare pupils through ICT for a rapidly changing world in which many activities are transformed by access to a varied and constantly changing and developing technology.

106. Pupils use ICT tools to find and process information and teachers need to set an example of how this is done in a responsible manner, creatively and with discrimination. Pupils learn from teachers how to employ ICT to enable rapid access to ideas and experiences from a wide range of sources. All staff need to become confident users of ICT, so that they can develop the skills, knowledge and understanding which enables them to use appropriate ICT resources effectively as powerful tools for teaching. This will support the way in which students successfully and safely engage with ICT resources in school.

107. ICT is also a vital tool in the administration of the school. Teachers and support staff need to be aware of what is acceptable use of the school's administrative network of computers.

108. **At The Tiffin Girls' School ALL OUR SYSTEMS ARE CLOSELY MONITORED**

Introduction

109. This section of the E-Safety Policy is in place for use of these ICT facilities by staff. There is a separate section in the policy for use by pupils.

110. There is a small network of computers which are used in the administration of the school (finances, pupil records, timetables, registers etc.). Many more computers are available for use by pupils and staff and the majority of these have access to the internet through the school network. All pupils and staff have a login name, password and an email account.

111. The email system is available for use both from within the school and externally using a web browser.

112. There are specialist classrooms serving design, mathematics and science together with general purpose rooms. A growing number of other computers are located within individual departments/classroom areas.

113. The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:
    - Users can only access data to which they have right of access.
    - No user should be able to access another's files without permission (or as allowed for monitoring purposes within the school's policies).
    - Access to personal data is securely controlled in line with the school's personal data policy.
    - Logs are maintained of access by users and of their actions while users of the system.

Objectives and targets

114. This policy sets out the code of practice for use of ICT by staff at The Tiffin Girls' School.

Action plan

115. The following code of practice must be adhered to by staff.

116. All staff will be expected to sign the ICT: Staff acceptable usage agreement – see appendix 5. Staff who receive a laptop which is the property of the school will also be expected to sign the ICT: Staff acceptable laptop usage agreement – see appendix 6.

Rights of access

117. A safe and secure username/password system is essential and will apply to all school ICT systems, including email and managed learning environment (MLE).

118. All passwords are generated by the network manager/ICT technical support staff and are unique to each member of staff. Passwords can only be reset by the user or by the ICT technical team. All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the network Manager and these will be reviewed, at least annually.

119. The "master/administrator" passwords for the school ICT system used by the network manager/ICT technical support team are also available to the Headteacher or other nominated senior leaders and kept securely. In the event of a serious security incident the police may request, and will be allowed access to, passwords used for encryption.

Emails

120. The computer resources at The Tiffin Girls' School belong to the school and are to be used solely for educational or business purposes.

121. Email is an essential tool at the school and all members of staff should use their professional judgement whilst using email as a means of communication. See Appendix 7 for further guidance.

Internet and intranet (see Staff Code of Conduct for further guidance)

122. The internet is not necessarily secure and school sensitive information could be viewed by unauthorised individuals.
    - Staff must abide by the current restrictions on correspondence or the passing of information to outside organisations or individuals.
    - The transmission of school sensitive data over the internet is strictly prohibited unless via secured and encrypted connections
    - At no time may staff use the internet to send school or personal information that would, if intercepted, place the school in violation of UK laws or regulations.
    - Staff may not use the internet to view illegal, pornographic or seditious material.
    - Staff may not download or distribute material from the internet without virus checking.
    - Staff may not use the internet in a role inconsistent with their role in the school.
    - Staff must not gain unauthorised access to the internet e.g. by hacking or by trying to circumvent any 'blocking' controls.
    - Staff must not use another individual's user identity to access the internet or intranet.
    - Staff may not download screensavers, sounds, images, or audio-visual materials for storage on local PCs.
    - Staff may not use the internet for private business purposes or private commercial gain.

- Staff must not engage inappropriately with pupils through social networking sites. Staff must be mindful that all postings on social network sites are widely accessible

Laptop computers and other devices

123. Laptops, ipads, tablets, smart phones and similar devices which are used on the school network fall under the same restrictions of use as networked computers. Loss, damage or theft of a school laptop through misuse, or negligence may result in financial sanctions.

124. The use of personal devices should adhere to the school's Staff Code of Conduct policy and model best practice. Their use should be limited to non-student contact time and reflect the school rules for students' use of mobile devices around the site.

125. Laptops and peripherals should be kept in a secure place and transported in the car boot. When not in use, the laptop should be switched off and kept in its case.

Web filtering

126. Requests for currently blocked sites to be made accessible on our network should be made to the ICT Services Manager via email which includes a link to the site requested and outlines the educational rationale for access to the website.

127. The ICT Services Manager will pass this onto a member of the Senior Leadership Team ('SLT') responsible for pastoral care.

128. The SLT member will evaluate the site and decide whether access should be allowed and will communicate this to the member of staff who made the request and the ICT Services Manager.

129. The SLT member will discuss with other members of SLT and seek expert advice if necessary.

130. The decision to allow access to a website can and will be reversed should it be deemed necessary by the SLT.

Remote Access

131. Approval for the installation of a VPN link will be at the discretion of the School.

132. Only software authorised for the purpose of connecting to the school's network via a LGfL (Rav3) VPN tunnel may be used.

133. The authorised software may be installed only on equipment (school or private) approved for that purpose by the school.

134. The installation of the software will be performed only by an authorised member of IT Technical team.

135. VPN users will be required to change security settings on their link when asked to do so by IT Services Manager.

136. All costs (e.g. ISP and telephony costs) incurred in using the VPN tunnel will be the responsibility of the end user.

137. It is the responsibility of staff and students with VPN privileges to ensure that unauthorized users are not allowed access to the network, i.e. the tunnel link is established for the sole use of the authorised user.

138. All computers connected to the network via VPN must use anti-virus software and maintain up-to-date virus definition files. In the case of private PCs this is the responsibility of the owner.

139. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of TiffNet while connected, and as such, subject to the terms of the Acceptable Use Statement.

140. Any member of staff or student found to have violated this policy may be subject to disciplinary action.

Misuse of computer systems by staff

141. Misuse or abuse of computer systems by staff is a serious matter and will be dealt with under the school's disciplinary procedures. The penalties for improper use may include dismissal, either with, or without notice. The following are expressly prohibited:
    - The unauthorised export or transmission of school software via the internet.
    - The accessing, viewing, downloading or forwarding of pornographic material or material of a racist or inflammatory nature.
    - The loading, downloading or forwarding of games software.
    - The generation or forwarding of 'chain' messages or letters.
    - The sending or forwarding of abusive or offensive emails – inside or outside the school – or material that could cause offence. This applies to all email, whether intended for person-to-person communication or wider distribution.
    - The list may be added to at any time. Known pornographic sites on the internet will be blocked and filters to intercept prohibited material and offensive language are in place. The school reserves the right to intercept, monitor, analyse and read all email generated, received or distributed via the school networks, equipment and email addresses.
    - Some email systems have the capability to send the contents of messages to fax machines. This policy applies equally to such messages and documents.

142. Any queries regarding this policy should be addressed to the Assistant Headteacher (Academic Progress, tracking & enrichment).

Monitoring and evaluation

143. All use of the internet is recorded and the Senior Leadership Team may request access to internet logs, emailing history etc. if the senior management team considers that this policy has been contravened, in order to investigate alleged abuse. The policy itself will be monitored and evaluated regularly taking into account any incidents which occur or technological developments which might need a change in the policy.

APPENDIX 5

ICT: Staff acceptable computer usage agreement

- I will only access the system with my own name and registered password.
- Passwords that I use to access school systems will be kept secure and secret.
- If I have reason to believe my password is no longer secure I will change it immediately. I will inform the network manager as soon as possible so that any access with my old password can be monitored and appropriate action taken.
- I acknowledge that the computer/laptop provided for me to use remains the property of the school and should only be used for school business.
- I will not access the files of others or attempt to alter the computer settings.
- I will not update web logs or use pictures or text that can identify the school.
- I will not alter, attempt to repair or interfere with the components, software or peripherals of any computer that is the property of the school.
- If I use removable media I will ensure that it is free from any type of virus.
- I will follow the guidance provided by ICT support staff to ensure the anti-virus protection on my laptop is kept up-to-date.
- I will check with the network manager/technician should I need to install additional software.
- I will always adhere to the following associated school policies:
    - E-safety: Staff professional identity policy
    - E-safety: Secure data handling policy
    - E-safety: Use of the network by staff
    - ICT: staff acceptable laptop agreement
- I will always adhere to copyright laws.
- I will always log off the system when I have finished working.
- I understand that the school does monitor the internet sites I visit.
- I understand that a criminal offence may be committed by deliberately accessing internet sites that contain certain illegal material.
- I understand that staff are not permitted to access social media websites from the school's computers, staff laptop or other school device at any time unless authorised to do so by a member of the senior management team.
- I will not open email attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the network manager as appropriate.
- Any email messages I send will not damage the reputation of the school.

- I will include the following disclaimer as part of an automated email signature in all emails sent to an external recipient from a school account:

  Please note that this email and any attachment(s) to it are confidential. Unless you are the intended recipient, you may not use, copy or disclose either the message or any information contained in the message. If you are not the intended recipient, please notify me immediately and delete this email. Thank you.

- I will report immediately to my line manager any unpleasant material or messages sent to me.

- I understand that use of the school's equipment for personal financial gain, gambling, political purposes or advertising is forbidden.

- I understand that the use of personal mobile devices should be restricted to during non-teaching/student contact time

- I understand that activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.

- I understand that I am responsible for the safety of sensitive school data that I use or access, including the use of cloud based applications.

- In order to maintain the security of data I will take the following steps:

  - I will store data files in my user area only for as long as is necessary for me to carry out my professional duties.
  - I will not share or give out any passwords that I use to access school systems. If I have reason to believe that my password is no longer secure I will change it.
  - If I am in any doubt as to the sensitivity of data I am using I will refer to the school's Secure Data Handling policy to check. Sensitive data could include:

    - Pupil reports.
    - SEN records.
    - Letters to parents.
    - Class-based assessments.
    - Exam results.
    - Whole school data.
    - Medical information.
    - Information relating to staff e.g. performance reviews.

I understand that if I do not adhere to these rules outlined in this agreement, my network access could be suspended, my laptop removed if relevant, and that other disciplinary consequences may follow.

If an incident is considered to be an offence under the Computer Misuse Act or the Data Protection Act this may require investigation by the police and could be recorded on any future criminal record checks.

Name…….. PLEASE PRINT

Signed:…… Date……..

APPENDIX 6

ICT: Staff acceptable laptop/mobile device usage agreement

- The laptop/device is the property of The Tiffin Girls' School. It has been allocated to me as a member of staff and is my responsibility. If another member of staff borrows it, the responsibility still stays with me and I understand that only school staff may use the laptop.
- I understand that students must never use the laptop/device.
- When I leave the school's employment, the laptop/device will be returned to the school.
- I understand that when in school and not being used, the laptop/device must be kept secured in an office, locked room or drawer. It must not be left in an unlocked, unattended classroom.
- I understand that, whenever possible, the laptop/device must not be left in an unattended car. If there is a need to do so, it will be locked in the boot.
- I will check that the laptop/device is covered by my normal household insurance. If this is not the case, then either the insurance must be changed or the laptop/device should be kept in school and locked up overnight.
- I understand that the laptop/device must not be taken abroad, other than as part of a school trip
- I understand that when being transported, the carrying case supplied must be used at all times.
- I understand that I have the responsibility to ensure the virus protection software that has been installed on the laptop/device is kept up-to-date. I also understand that I must *always* follow the virus protection procedures as directed by the school's technical support provider/network manager to ensure virus protection is always kept up-to-date.
- I understand that I should not attempt to significantly alter the computer settings other than to personalise my desktop working area.
- I understand that if I use any removable medium then it must be checked to ensure it is free from any viruses.
- If any fault occurs with the laptop/device I will refer it immediately to the technical support staff/network manager.

Laptop/device issued to:

Name……. PLEASE PRINT

Signed:……

Date……..

APPENDIX 7: GUIDE TO USING EMAIL

Introduction

Email can be a tremendously effective way of sharing information and managing work across an organisation. But email is only as good as the thinking and the practical organisation of the people using it. Badly used, it can clog up people's time and systems, cause upset and even cause offence.

Once an email is sent it is outside the control of the sender and can be copied to multiple recipients in a moment. Don't make the mistake of thinking your e-mails are private. They're not. Think of them as postcards. You should never include any information in an e-mail that you wouldn't want published on the front page of your local newspaper. In other words, never send confidential, proprietary, sensitive, personal, or classified information through e-mail. You should also avoid making inflammatory, emotionally charged comments in e-mail.

Know when to use e-mail (and when not to). Businesses provide e-mail for professional, business-related use, not for jokes, gossip, or chain e-mails. Also remember that you shouldn't send an e-mail to do a conversation's work. Complicated subjects are often difficult to explain face to face, much less in an e-mail. Consider setting up a short meeting to address the issue in person.

E-mail is also a poor stand-in for conversation when conducting critical, difficult, and/or unpleasant discussions, such as issues related to human resources matters. Sensitive communications are best handled in person.

Aim:

The aim of issuing guidance on email use is to improve the way that people communicate at school. However, an email policy helps only if people think about and apply the guidelines sensibly in their working lives.

The guidance is not a formal code that applies to the use of email at The Tiffin Girls' School, but a set of good practice guidelines. The guidance sets up expectations about how email should be used for good communication, but does not alter the policy for use of the internet/intranet by staff.

At the heart of good email practice is this: think clearly about why you are sending the email and what you are asking people to do.

A. Reducing the number of emails in circulation

Do you want to reduce the number of emails you get? A good start is to reduce the number you send.

- Think before you send an email. Is it the best way to communicate? Would it be better to phone or meet in person?
- Restrict your use of email mailing lists to messages about school business.
- Think before replying to or forwarding an email. Do you really need to reply at all or send it on?
- If you find yourself getting into a repetitive email dialogue, consider two things: cut out copy recipients, and try speaking in person instead.
- Make sure that people copied in actually need to know what is being sent. Email makes copying messages too easy: don't copy people in "just in case".

- When replying, don't send a "reply to all" unless it is necessary for all copy recipients to know your response.
- Unless the email asks for an acknowledgement, don't send one.

B. Create the right impression

- Make sure you follow proper grammar and sentence structure when composing and responding to messages and use a spell checker. It's easy to convey the impression that you're unprofessional or careless if you don't follow some basic principles of good business writing.

- Before clicking the Send button, give it a final once-over. Reread the entire e-mail, checking it for grammatical errors, punctuation mistakes, and typos.

- Also make sure your tone is appropriate.

C. Send emails to the right people

- Mailing lists provide useful groupings to target messages to the right groups of people. But don't misuse mailing groups by emailing with a 'scattergun' approach.
- Make clear if you are sending an email to a person in their role, e.g. as 'head of department'. That will help them to organise and manage emails.
- Don't use recipients as post boxes. People should be asked to cascade information only if they themselves need to know the information first, or have useful context to add in sending it on to their teams.
- If you want all staff in a certain department to receive an email, use the appropriate mailing list or speak to the head of the unit and see what the most effective communication route is.

D. Make email content and action clear

- Keep the subject line short and don’t write it in capitals.
- Make clear in the subject title of the email exactly what the subject is. Avoid multiple topics in the body of the message that don't match the title.
- The expectation is that emails are being sent "to" people who must take some sort of action. The "cc" is for people who need to know about this. Anyone else shouldn't be included.
- Do not cc someone’s line manager in order to put pressure on or imply criticism of the recipient. Do not use “cc” as a way of trying to influence others to take your point of view.
- Only use “bcc” in order to include the bcc recipient for information. Anyone who is included as “bcc” should not be surprised by the email.
- Make clear whether the email is sent for action or information and what the recipient is being asked to do and by when.
- If you really need to know an email has been received and read, ask for confirmation.
- Give contact details at the base of the email so people are clear who you are and can contact you, other than by email. These contact details should include job title and phone number.

E. Forwarding and replying to emails

- Respect the privacy of the email. It may contain information that is confidential or intended for you only.
- Be very careful about email threads. Always re-read the whole thread before sending on, or delete it. There may be an email embedded in the thread that was not intended for a later recipient to read.
- Think very carefully before you forward emails that you have received. Don't forward an email unless the original sender would want you to e.g. because they haven't got the email address of someone. Remember the original sender could have included the person you are forwarding to in the first place. If in doubt check. Never forward and email from your line manager unless expressly requested to do so.
- When replying to email, try to scan the reply to eliminate unneeded text such as repeat addresses. Include your signature immediately below the text you are writing. Consider using a different colour font if possible to show your comments.
- When forwarding or replying to emails, follow the same rules as you would for initiating an email, e.g. make clear to whom you are sending it and what action is needed. Also make sure the subject is the appropriate one.

F. Managing your own emails

- Consider working on email only at set times during the day. Even if you don't, make allowance for people who do this: don't expect instant replies.
- Think carefully about when you send emails, particularly if it is not during working hours or late at night. Save and send the next morning, especially if it is to colleagues you line manage.
- When you are on leave or unable to read email, set-up an auto-reply message. That information should make clear who can be contacted in your absence.

G. Email writing style

- Keep messages short, warmly professional and to the point.
- Keep paragraphs and sentences short: they are easier to read.
- Do not treat email like spoken communication. Email is a more informal medium than memos or letters, but it lacks the signals and cues that spoken language contains.
- Avoid using UPPER CASE, as it looks as if you are SHOUTING. Use bold, underline or italics for emphasis.
- Once drafted, re-read your email before you press 'send'. Think about how it could come over to the recipient.
- Never send an email when you are upset or angry, even if an email has caused that feeling. Never respond to bad email etiquette like for like.

H. Using email to send documents

E-mail attachments can consume inordinate amounts of e-mail server space and network bandwidth and can be the culprits behind virus outbreaks--but they're often the easiest way to transfer files. Follow these guidelines when e-mailing attachments:

- Don't attach large files to an e-mail; anything over one or two megabytes shouldn't be sent via e-mail.

- Limit the number of files you attach to a message to five or fewer.
- Don't open unexpected attachments or those sent by unknown parties.
- Don't annoy recipients by forwarding attachments they can't access. If an attachment requires a new or less-common application, say so in your message.
- Unless they are genuinely urgent, consider sending formal documents in hard copy. People get exactly what you want in the right order and may well be more likely to read, digest and understand what you are saying.
- Think before you send something short as an attachment. It may be more effective to put the content in the email itself so that recipients can read it easily.
- If you have to send attachments, identify as clearly as possible what attachments are being sent.

I. Legal issues and email

- Note that emails sent from a Tiffin Girls' School email address carry the same authority as letters sent on the school letter-headed paper.
- Remember that the school has the right to access all emails sent and received by school email accounts
- Laws relating to written communications apply to email messages.
- Email should not be used for frivolous, abusive or defamatory purposes: emails are actionable within the laws of defamation.
- Emails can constitute harassment and be used as evidence of such.
- Where the school detects abuse or inappropriate use it will take action to address it.

J. Security issues

- Unless using encryption techniques, all email is insecure. Anything you record in an email may be read by others. Take great care when considering sending out personal, confidential or sensitive information by email. All email sent to an external recipient from a school account should have, as part of an automated email signature, the following disclaimer in 7.5pt font:

  Please note that this email and any attachment(s) to it are confidential. Unless you are the intended recipient, you may not use, copy or disclose either the message or any information contained in the message. If you are not the intended recipient, please notify me immediately and delete this email. Thank you.

- Unless you are certain about the authenticity of an email, do not act on its content as it could contain a virus or be fraudulent.
- Never disclose confidential information - such as passwords - in response to an email message. Ensure that you comply with the school's E-safety: Secure Data Handling policy.