TAVERHAM
Junior School

'Learning for a fuller life...'

E-Safety Policy

As a Church of England school, we see it as our duty to give children and members of the school community the skills to maximise their engagement with the world around them, enable them to grow spiritually, emotionally and personally, and develop the character and values which will serve them well in future life and support success.

Introduction

1. The E-safety Policy relates to other policies including those for ICT/computing, bullying and for safeguarding/child protection.
2. The school will identify a member of staff who has an overview of E-safety, this would usually be the Safeguarding Lead and/or a member of the SLT
3. Our E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior staff and approved by governors.
4. The E-safety Policy and its implementation will be reviewed annually
5. The original policy was approved by the Governors on 17.11.14. The most recent review was agreed on 19.6.17
6. The school Internet access is provided by Updata and includes filtering appropriate to the age of pupils. However, we understand that no amount of filtering will guarantee that inappropriate content will never be accessed by children in school and that it is vital that children know they are responsible in reporting inappropriate images/sites that they or others may access on the internet (whether in school or at home).
7. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
8. Pupils will be educated in the effective use of the Internet
9. Pupils will be shown how to publish and present information appropriately to a wider audience.
10. Pupils will be taught how to evaluate Internet content
11. The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
12. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
13. Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

Information system security

14. School ICT systems security will be reviewed regularly.
15. Virus protection will be updated regularly.
16. Security strategies will be discussed with the Local Authority.

E-mail

17. Pupils and staff may only use approved e-mail accounts on the school system.
18. Staff should only use work (i.e. 'head@', 'office@' 'nsix' etc) email addresses to communicate with parents
19. Pupils must immediately tell a teacher if they receive offensive e-mail.
20. Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
21. Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.
22. Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
23. The school will consider how e-mail from pupils to external bodies is presented and controlled.

Published content and the school web site

24. The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
25. ***JACOB MERRILL*** will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing photographs, images and work

26. Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs rather than full-face photos of individual children.
27. Pupils' full names will be avoided on the website or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
28. Written permission from parents or carers will be obtained before photographs or images of pupils are published.
29. Written permission from adults will be obtained before their names, photographs or images of themselves are published.
30. Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing on the school learning platform

31. The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords.
32. All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location.
33. Pupils must not place personal photos on any social network space provided in the school learning platform without permission.
34. Pupils, parents and staff will be advised on the safe use of social network spaces.
35. Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing filtering

36. The school will work in partnership with Norfolk Children's Services to ensure systems to protect pupils are reviewed and improved.
37. If staff or pupils come across unsuitable on-line materials, the site must be reported to the nominated member of staff.
38. The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

39. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Other devices

40. Pupils are permitted to bring mobile phones into school but these should not be switched on or used on school premises.
41. Staff should not use personal devices to take pictures of children
42. Class iPads and mini iPads can be used to take photos of children (whose parents have signed consent) to record/support learning and to celebrate success or promote the school etc.
43. The sending of abusive, offensive or inappropriate material is forbidden.

Protecting personal data

44. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet access

45. All new staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource. (Existing staff have already done so)
46. Pupils must agree to comply with the Responsible Internet Use statement before being granted Internet access.
47. Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' form before being allowed to access the Internet on the school site.

Assessing risks

48. The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Norfolk Children's Services can accept liability for the material accessed, or any consequences of Internet access.
49. The school will review ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

Handling E-safety complaints

50. Complaints of Internet misuse will be dealt with by a senior member of staff.
51. Any complaint about staff misuse must be referred to the headteacher.
52. Complaints of a child protection nature must be referred to one of the school's Safeguarding Leads and dealt with in accordance with school child protection procedures.
53. Pupils and parents will be informed of the complaints procedure.
54. Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

55. All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety policy.

Introducing the E-safety policy to pupils

56. Appropriate elements of the E-safety policy will be shared with pupils
57. E-safety rules will be posted in all networked rooms.
58. Pupils will be informed that network and Internet use will be monitored
59. Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils on at least a half-termly basis. The Deputy Head leads a whole school E safety assembly every term.

Staff and the E-safety policy

60. All staff will be given the School E-safety Policy and its importance explained
61. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
62. Staff who manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues**.**
63. All school staff should make reference to the school's ICT Code of Conduct, and to Norfolk CC's Employee Code of Conduct (G303c) and 'Internet, social networking and email policy' (P319).

Involving Parents *(was 'enlisting parents' support')*

64. Parents' and carers' attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school website.
65. Parents and carers will from time to time be provided with additional information on E-safety.
66. The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
67. Parents will routinely be contacted whenever there is an E safety issue involving their child, whether in school or outside school, when an incident outside school has been brought to the school's attention by other parents or pupils.
68. The police, safeguarding adviser and/or CEOP may be involved if there is a serious breach of E safety by any pupil.

Governors will regularly review the effectiveness and impact of this policy through conversations with pupils and staff.

Appendix to Computing policy

The Acceptable Use Policy/Code of Conduct: All adults working in school.

Please refer to the Norfolk County Council document P319 'Internet, social networking and email policy' (P319).

For personal use:

1. Do not give anyone access to your login name or password.
2. Do not open other people's files without express permission. Do not corrupt, interfere with or destroy any other user's information.
3. Do not release personal details including phone numbers, fax numbers or personal e-mail addresses of any colleague or pupil over the internet.
4. Do not reproduce copyright materials without first getting permission from the owner. Many people will make their work available for education on request. Acknowledge sources on all resources used.
5. Do not attempt to visit sites which might be considered inappropriate. All sites visited leave evidence on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.
6. Use of school internet access for business, profit, advertising or political purposes is strictly forbidden.
7. Users should log out and close their browser when they have finished.
8. Do not write or post information on social networking sites which contains direct reference to any pupil at TJS. On social networking sites, staff should ensure that their personal profile is set to the highest security setting available and that they are not 'friends' and do not have contact with pupils, ex-pupils or parents. Staff are reminded that any action or comment that brings the school or colleagues into disrepute or compromises pupil or staff confidentiality will be classed as a disciplinary matter.
9. Do not post anything on a social networking site, blog or VLE which is likely to cause annoyance, inconvenience or needless anxiety.
10. Be mindful of content posted on blogs or social networking sites that may be available to view by parents or other third parties. Never engage in conversation online that contains direct reference to individual pupils or contains sensitive material or judgements/opinions about school related issues.

Blogs

11. Only post material that is intended for educational use or to showcase educational content from pupils.
12. Be respectful and polite when commenting on work or materials posted by staff or children on learning platforms or blogs.
13. Be aware of children whose parents have not given permission for their photographs to be used online and ensure that their wishes are adhered to.
14. Do not post children's surnames or personal details on class blogs.
15. Report any concerns with material posted by others to senior management or the ICT co-ordinator.
16. Ensure sensitive materials are locked down to be available only to relevant individuals. Seek advice from ICT team when unsure.

Personal E-mail

17. Follow school guidelines contained in the ICT policy for the use of e-mail.
18. Observe *netiquette* on all occasions. E-mail should not be considered a private medium of communication.

19. Do not include offensive or abusive language in your messages or any language which could be considered defamatory, obscene, menacing or illegal. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority.
20. Make sure that nothing in your messages could be interpreted as libellous.
21. Do not send any message which is likely to cause annoyance, inconvenience or needless anxiety.
22. Do not send any unsolicited promotional or advertising material nor any chain letters or pyramid selling schemes.

When using the internet, learning platform, blogs or e-mail with children.

23. Remind children of the rules for using the internet, learning platforms or e-mail.
24. Watch for accidental access to inappropriate materials and report the offending site to the designated professional.
25. Check before publishing children's photographs; make sure that you have parental permission.
26. Ensure that children comment respectfully on other's work or blogs.
27. Follow up any inappropriate behaviour with the headteacher.
28. Report any breaches of the schools internet policy to the designated professional.
29. The school will periodically check the use of school computers and the internet to check that all use has been appropriate.