



ARCHBISHOP SANCROFT HIGH SCHOOL ICT & E-SAFETY POLICY

Reviewed by:	Head Teacher, ICT Co-ordinator, Link Governor ICT
E-Safety Co-ordinator:	ICT Co-ordinator
Norfolk Policies Links:	Children's Services E-Safety Policy; Norfolk County Council Code of Use and Code of Connection Policies, Data Protection
School Policy Links:	Behaviour; Anti-Bullying; Confidentiality; Data Protection; Data Retention; Safeguarding; Whistle blowing; Child Protection

Notes:

The E-Safety Policy also includes a number of Appendices. These may refer to the Norfolk E-Safety Policy and in addition include various documents used as part of the school's E-Safety Strategy. In addition it will contain policy documents which define the management of the school network in order to comply with requirements for the security of the network.

These are:

Appendix A	Norfolk Children's Services ICT Policy
Appendix B	Password Policy
Appendix C	Backup Procedure
Appendix D	Anti-virus Procedure
Appendix E	Staff Code of Conduct
Appendix F	Laptop Agreement
Appendix H	Sanctions for Student Misuse of the Network
Appendix I	Student Acceptable Use Policy/Home Agreement

Still in preparation by Norfolk Children's Services and to be possibly added as part of the E-Safety Policy in the future:

1. Parental e-Safety Rules of Consent
2. E-Safety Contacts and References
3. E-Safety Legal Framework
4. E-Safety Process: Response to an Incident
5. E-Safety Photo Guidance



1 PRINCIPLES

Our e-Safety Policy has been written by the school, building on the NCC e-Safety Policy and government guidance. It has been agreed by the senior management and approved by governors. We believe that staff and students at Archbishop Sancroft High School have the right to work and study using the Internet & ICT resources in a safe learning environment. Access to these resources must be within the law.

- 1.1 The school will appoint an E-Safety Co-ordinator (J Cracknell, ICT Co-ordinator)
- 1.2 The E-Safety Policy and its implementation will be reviewed annually.

2 PURPOSES

- 2.1 The policy defines and describes the use of the ICT network and electronic information to support, enhance and develop all aspects of the curriculum at Archbishop Sancroft High School.
- 2.2 To ensure that all users have full use of all resources allocated to them from any computer within their scope of access.
- 2.3 To ensure that all users are able to access the Internet in order to support and promote learning.
- 2.4 To provide all users with a secure environment in which to use network and Internet resources.

3 OBJECTIVES AND SCOPE

The primary objectives of this policy are:

- 3.1 to safeguard ICT resources and the integrity of data stored on the network.
- 3.2 to minimise the liability arising from the misuse of ICT resources and data
- 3.3 to ensure that the confidentiality of data is protected to the extent allowed or required by all laws pertaining to it
- 3.4 To comply with the Norfolk County Council & Children's Services E-Safety Policies and Requirements
- 3.5 The policy detailed here applies to the use of all ICT resources and data and is applicable to all staff and students of Archbishop Sancroft High School, and all other authorised users.

4 RESPONSIBILITIES

- 4.1 All ICT systems, resources & data are the property of Archbishop Sancroft High School and Norfolk County Council, including laptops & mobile computing devices, software, operating systems, storage media and network accounts that provide access to local, network, Internet and email resources
- 4.2 ASHS will ensure that all users are fully aware of the contents contained within this policy.
- 4.3 The ICT Department is responsible for granting access to ICT resources allocated to staff and students in accordance with their role within the school. Any deviation from this must be authorised by the Headteacher.
- 4.4 File quotas will be imposed on users. No staff or student user will be allowed unlimited quota in order to make sure one person does not fill the entire file storage area & so bring the network to a halt.
- 4.5 When a breach of this policy is reported, the incident will initially be reviewed by the Systems Engineer or ICT Co-ordinator and passed to either the E-Safety Co-ordinator (students) or Head Teacher (students/staff) for further review in accordance with the Pupil Behaviour



5 USER RESPONSIBILITIES

5.1 When using computer network and Internet resources all users must comply with all laws pertaining to their access, including copyright, libel, fraud, discrimination and obscenity laws.

5.2 All breaches of this policy must be reported to the Systems Engineer/E-Safety Co-ordinator in the first instance.

5.3 By logging onto or using any ICT resource belonging to or within the boundaries of ASHS, users agree to abide by this policy and all policies and laws relating to the use of ICT.

5.4 All staff and students are to act in a responsible, lawful and ethical manner. Staff must be aware that all data including electronic email and documents stored on the system may be accessible to the public under the Freedom of Information Act 2000.

5.5 All users must agree to comply with the law in the use of the ICT system.

5.6 All users are to ensure that their password is not shared or compromised, nor use another users account or attempt to access another user account. If a user's password is found to be compromised, it is the responsibility of the user to ensure that their password is changed.

5.7 Users shall not access another users personal electronic documents (email included) without the owners express permission or as allowed by law

5.8 Staff are to ensure that no computer resource allocated to them is left unsecure where there is student access

5.9 No person may knowingly:

5.9.1 Connect a device to the network or any ICT resource without prior approval, this includes VOIP phones, laptops, PDA's, Gaming devices, mobile phones

5.9.2 Play online computer games or use interactive 'chat' sites unless specifically approved by the school.

5.9.3 Access social networking sites unless specifically approved by the school

5.9.4 Use the network in such a way that the use of the network by other users is disrupted (for example: downloading large files during peak usage times; sending mass email messages).

5.9.5 Retrieve, send, copy or display offensive, pornographic, obscene or racist messages or pictures.

5.9.6 Use obscene or racist language, or harass, insult or attack other people

5.9.7 Damage computers, computer systems or computer networks.

5.9.8 Use another user's password.

5.9.9 Create or transmit any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;



- 5.9.10 Create or transmit defamatory material
 - 5.9.11 Corrupt or destroy other users' data;
 - 5.9.12 Disrupt the work of other users;
 - 5.9.13 Introduce or attempt to introduce a "virus".
 - 5.9.14 Attempting to bypass network or computer security including Antivirus Software, using programmable scripts or network monitoring software.
 - 5.9.15 Attempt to gain access to or use resources NOT allocated to them
 - 5.9.16 Download programs without approval from the Systems Engineer or ICT Co-ordinator
 - 5.9.17 Use Peer to Peer file sharing programs (Kazaa, Emule, BitTorrent etc)
 - 5.9.18 Use MSN, Yahoo, AOL Messenger or other types of chat programs whilst connected to the school network, unless the service is approved by ICT Co-ordinator or /Head Teacher as some methods might be appropriate for a managed learning environment.
- 5.10 Users should:
- 5.10.1 Inform the E-Safety Co-ordinator if they believe that attempts have been made to use the Internet in an unacceptable manner
 - 5.10.2 Inform the E-Safety Co-ordinator if they discover any materials they consider may be offensive or inappropriate

6. How can we safely use the Internet to enhance learning?

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the needs of the curriculum. A different level of filtering may be provided for staff in order for them to carry out their professional duties. Staff should not allow students to use this filtering level as they may access resources inappropriate for their age.

- 6.1 Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- 6.2 Internet access will be planned to enrich and extend learning activities.
- 6.3 Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- 6.4 Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- 6.5 Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- 6.6 E-Safety should be embedded into the curriculum for all departments.

7. How will pupils learn how to evaluate Internet content?

The quality of information received via radio, newspaper and telephone is variable and every student needs to develop skills in selection and evaluation. Information received via the Internet, e-mail or text message requires good information handling skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues present with books or TV may be missing or difficult to read. In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the



page and report the incident immediately to the teacher.

More often, pupils will be judging reasonable material but will need to select relevant sections.

Pupils should be taught research techniques including the use of subject catalogues and search engines and be encouraged to question the validity, currency and origins of information. Key information handling skills include establishing the author's name, date of revision and whether others link to the site. Pupils should compare web material with other sources. Effective guided use will also reduce the opportunity pupils have for exploring unsavoury areas.

Clearly pupils need to understand that unselective copying is worth little without a commentary that demonstrates the selectivity used and evaluates significance. Respect for copyright and intellectual property rights, and the correct use of published material should be taught. Methods to detect plagiarism may need to be further developed and are certainly part of examination boards' thinking.

7.1 The schools will endeavour to ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

7.2 The following statements require adaptation according to the pupils' age and understanding:

7.2.1 Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

7.2.2 Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

7.3 The evaluation of on-line materials is a part of every subject when they are being used.

8 Managing Information Systems

How will information systems security be maintained?

8.1 Users must act reasonably – e.g. the downloading of large files during the working day or listening to online radio stations/streaming of multimedia will affect the service that others receive.

8.2 Users must take responsibility for their network use. Breaching the Staff Code of Conduct ICT policy may result in disciplinary action.

8.3 Workstations should be secured against user mistakes and deliberate actions. Servers must be located securely and physical access restricted where possible.

8.4 The server operating system must be secured and kept up to date.

8.5 Virus and Spyware protection will be installed and updated regularly.

8.6 Access by wireless devices must be pro-actively managed.

8.7 Wide Area Network (WAN) security issues include:

8.7.1 All Internet connections must be arranged via the Norfolk County Council Children's services to ensure compliance with the security policy.

8.7.2 NCC firewalls and switches are configured to prevent unauthorised access between schools.

8.7.3 Decisions on WAN security are made on a partnership basis between school and NCC.

8.8 The security of the school information systems will be reviewed regularly by an ICT Working Party. Virus and Spyware protection will be installed and updated regularly.



- 8.9 Security strategies will be discussed with ICT Solutions.
- 8.10 Login details must not be shared
- 8.11 Personal data sent over the Internet will be encrypted or otherwise secured.
- 8.12 Unapproved system utilities and executable files will not be allowed in work areas or attached to e-mail.
- 8.13 The Systems Engineer will review system capacity regularly and will report to the ICT Working Party.
- 8.14 Automatic updates will be applied to keep all workstations secure & up to date. This should be managed centrally.

9. How will e-mail be managed?

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between schools in neighbouring villages and in different continents can be created.

When using email for teaching, the implications of e-mail use for the school and pupils need to be thought through and appropriate safety measures put in place. Un-regulated e-mail can provide routes to pupils that bypass the traditional school boundaries and no information audit trail.

In the school context, e-mail should not be considered private and most schools and many companies reserve the right to monitor e-mail. There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

Spam, phishing and virus attachments can make e-mail dangerous. The Norfolk Schools Broadband Network and services provided on this network have security in place to reduce the impact of SPAM, phishing, viruses and other malware.

- 9.1 Pupils may only use approved e-mail accounts.
- 9.2 Pupils must immediately tell a teacher if they receive offensive e-mail. The teacher must inform the e-safety co-ordinator.
- 9.3 Users must not send jokes or other materials that the receiver may find offensive
- 9.4 Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- 9.5 Pupil access in school to external personal e-mail accounts should be blocked.
- 9.6 Excessive social e-mail use can interfere with learning and may be restricted.
- 9.7 E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- 9.8 The forwarding of chain letters is not permitted.
- 9.9 Email subscriptions to websites or other electronic services should be authorized by the ICT Co-ordinator for students.
- 9.10 No business contract should be made via email unless express permission is obtained from the Headteacher or Finance Officer (as appropriate).

10. Published content management

Many schools have created excellent websites that inspire pupils to publish work of a high standard. Websites can celebrate pupils' work, promote the school and publish resources for projects. Editorial guidance will help reflect the school's requirements for accuracy and good presentation.

Sensitive information about schools and pupils could be found from a newsletter but a school's website is more widely available. Publication of information should be considered from a personal and school security viewpoint. Material such as staff lists or a school plan may be better published in the school handbook or on a secure part of the website which requires authentication.



- 10.1 The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
- 10.2 E-mail addresses should be published carefully, to avoid spam harvesting by web crawlers
- 10.3 The head teacher or designated person will take overall editorial responsibility and ensure that content is accurate and appropriate.
- 10.4 The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

11 Can pupil's images or work and staff images be published?

Still and moving images and sounds add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount. Strategies include using relatively small images of groups of pupils and possibly even using images that do not show faces at all. "Over the shoulder" can replace "passport-style" photographs but still convey the educational activity. Personal photographs can be replaced with self-portraits or images of pupils' work or of a team activity. Pupils in photographs should, of course, be appropriately clothed.

- 11.1 Images of a pupil should not be published without the parent's or carer's written permission.
- 11.2 Pupils also need to be taught the reasons for caution in publishing personal information and images in social publishing sites
- 11.3 Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- 11.4 Pupils' full names will not be used anywhere on the website or blog, particularly in association with photographs.
- 11.5 Staff shall be able to opt out of having their picture published online.

12 How will social networking and personal publishing be managed?

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control.

For use by responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published.

Examples include: blogs, wikis, MySpace, Bebo, Piczo, Windows Live Spaces, MSN space, forums, bulletin boards, multi-player online gaming, chat rooms, instant messenger and many others.

- 12.1 The schools will have the option to block/filter access to social networking sites.
- 12.2 Newsgroups will be blocked unless a specific use is approved.
- 12.3 Pupils and staff will be advised never to give out personal details of any kind which may identify themselves or others and / or their location. (Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.)
- 12.4 Users should be advised to place only appropriate photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.
- 12.5 Teachers' official blogs or wikis should be password protected and run from the school website.
- 12.6 Teachers must not run social network spaces for student use on a personal basis' - 'However professional use may be encouraged if specific to a dedicated learning outcome i.e. utilising social networking technology to provide additional support to



students with their coursework. If doing so teachers need to ensure that pupils also create a 'professional' space for this purpose only

12.7 All users should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Users should be encouraged to invite known friends only and deny access to others.

12.8 Users should be advised not to publish specific and detailed private thoughts.

Staff should be aware of and deal with bullying that can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments. The inclusion of inappropriate language or images within text messages is difficult for staff to detect. Pupils may need reminding that such use is both inappropriate and conflicts with school policy. Abusive messages may be dealt with under the school bullying policy.

13. How will filtering be managed?

Levels of Internet access and supervision will vary according to the pupil's age and experience. Internet access must be appropriate for all members of the school community. Older secondary pupils, as part of a supervised project, might need to access specific adult materials; for instance a course text or set novel might include references to sexuality. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognized and restrictions removed temporarily.

The Norfolk Schools Broadband Network uses a centrally managed system for both Primary and Secondary school filtering. The system is called Bluecoat and it is an industry-standard system.

The school will work with ICT Solutions to ensure that systems to protect pupils are reviewed and improved.

13.1 The Head Teacher & e-safety/ICT co-ordinator will be made aware of filtering profile changes by ICT Solutions

13.2 If staff or pupils discover unsuitable sites, the URL must be reported to the e - Safety Co-ordinator and / or ICT Solutions.

13.3 Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

13.4 Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP and ICT Solutions.

14 How will videoconferencing be managed?

Videoconferencing enables users to see and hear each other between different locations. It is a 'real time' interactive technology and has many uses in education. This is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

Equipment ranges from small PC systems (web cameras) to large room based systems that can be used for whole classes or lectures. The videoconferencing equipment uses a 'network' to communicate with the other site.

All modern standards-based videoconferencing systems will connect over IP (Internet Protocol) . However, videoconferencing over the Internet, even with a broadband connection, can be unpredictable since it is a shared network and quality of service cannot be controlled. Schools using the Internet for videoconferencing should be aware that it is not managed by a single responsible agency and that there is no inherent security.

The National Educational Network (NEN) is a secure, broadband, IP network interconnecting regional schools' networks across England with the Welsh, Scottish and the Northern Ireland networks. Schools should use IP technology in a secure and managed environment.

The equipment and network

14.1 IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.

14.2 All videoconferencing equipment in the classroom must be switched off when



not in use and not set to auto answer.

- 14.3 Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- 14.4 External IP addresses should not be made available to other sites.
- 14.5 Videoconferencing contact information must not be put on the school Website.
- 14.6 The equipment must be secure and if necessary locked away when not in use.
- 14.7 School videoconferencing equipment must not be taken off school premises without permission. Use over the non-educational network cannot be monitored or controlled.

Users

- 14.8 Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- 14.9 Videoconferencing must be supervised appropriately for the pupils' age.
- 14.10 Parents and guardians must agree for their children to take part in videoconferences.
- 14.11 Responsibility for the use of the videoconferencing equipment outside school needs to be established using a risk assessment for the users.
- 14.12 Only key administrators should be given access to the videoconferencing system, web or other remote control page available on larger systems.
- 14.13 Unique log on and password details for access to JANET / UKERNA videoconferencing services should only be issued to members of staff and kept secure (if you are using the National Education Network) .

Content

- 14.14 When recording a videoconference lesson, permission should be given by all sites. The reason for the recording should be given and the recording of videoconference made clear to all parties by the start of the conference.
- 14.15 Recorded material shall be stored securely.
- 14.16 If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- 14.17 Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

15 Use of Mobile Phones

- 15.1 Mobile phones may be used as part of lessons or formal school time at the discretion of the Head Teacher. However, the sending of abusive or inappropriate text messages is forbidden and may be illegal.
- 15.2 Staff will be issued with a school phone where contact with pupils is required.
- 15.3 If contact with pupils is necessary staff must use school-owned equipment.
- 15.4 The inclusion of inappropriate language or images within text messages is difficult for staff to detect. Pupils may need reminding that such use is both inappropriate and conflicts with school policy. Abusive messages may be dealt with under the school bullying policy.



16 How can emerging technologies be managed?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, wide Internet access and multimedia. A risk assessment needs to be undertaken on each new technology and effective practice in classroom use developed. **The safest approach is to deny access until a risk assessment has been completed and safety demonstrated and contact made with the Transformation Technology Board.**
Contact: Business Support at ICT Solutions.

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

17 How should personal data be protected?

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Data Protection Act 1998 gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information is handled properly.

NCC Data Protection information may be seen at:

Norfolk schools web site <http://schools.norfolk.gov.uk/>

Commissioner's Office: <http://www.ico.gov.uk/>

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

17.2 The school will have a Data Protection Policy.

18 Policy Decisions

How will Internet access be authorised?

Internet access will be allocated on the basis of educational need. It should be clear who has Internet access and who has not. Authorisation is on an individual basis in a secondary school. For visiting groups Internet access will be granted where supervision is in place in the classroom.

18.1 The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

18.2 All staff must read and sign the 'Staff Code of Conduct for ICT' and read the guidance before using any school ICT resource.

18.3 Students must apply for Internet access individually by agreeing to comply with the e -Safety Rules.

18.4 ICT Co-ordinator/E-Safety Officer will deal with deciding which sites to block for student access and will have administrative access to block sites so this can be done immediately for child protection.

18.5 The Head Teacher, E-Safety Co-ordinator, ICT Co-ordinator will have administrative access to monitoring software. The Head Teacher may delegate the monitoring role to other members of staff.

19 How will e-safety complaints be handled?

Parents, teachers and pupils should know how to submit a complaint. The facts of the case will need to be established, for instance whether the Internet use was within or outside school.

19.1 Where necessary the complaints policy and disciplinary procedures will be followed.

20 How the Internet is used by the school in the community

Internet access is available in many situations in the local community as part of their education. In addition to the home and school, access may be available at the local library, youth club, adult education centre, village hall, supermarket or cyber café.

20.1 Students with outside access (e.g. on work experience) need to follow both the school's E-policy and any applicable to the placement.

20.2 We will liaise with other organisations where appropriate and the Children's Services e-Safety



Group to establish a common approach to e-safety.

20.3 We will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

21 How the Internet is used by the community in the school

21.1 Community users coming into schools must adhere to the school's E-safety policy.

22 Communications Policy

How will the policy be introduced to pupils?

A poster in every room with a computer will remind pupils of e-safety rules at the point of use.

22.1 E-Safety rules will be posted in rooms with Internet access.

22.2 Users will be informed that network and Internet use will be monitored.

22.3 The Head Teacher must ensure that an appropriate person attends an e safety training programme to raise the awareness and importance of safe and responsible Internet use.

22.4 Instruction in responsible and safe use should precede Internet access.

22.5 An AUP will be required to be agreed when accessing the computer network as a reminder. The frequency of notifications will be decided by the E-Safety Co-ordinator.

How will the policy be discussed with staff?

Staff must sign the Code of Conduct in relation to this policy. It is important that all staff feel confident to use new technologies in teaching. The School e-Safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies.

Staff must understand that the rules for information systems misuse for NCC employees are quite specific. Instances resulting in dismissal have occurred. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

ICT use is widespread and all staff including administration, caretaker, governors and helpers should be included in appropriate awareness raising and training. Induction of new staff and regular supply should include a briefing of the school's e-Safety Policy.

22.6 All staff will be given the School e-Safety Policy and its application and importance explained.

22.7 Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

22.8 Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

22.9 Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

22.10 All new Staff should have a briefing of the school's e-Safety policy by the e-safety co-ordinator before they have access to the ICT network.

How will parents' support be enlisted?

Internet use in pupils' homes is increasing rapidly, encouraged by offers of free access and continual media coverage. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet.

22.11 Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school website. Internet issues will be handled sensitively, and parents will be advised accordingly.

22.12 A partnership approach with parents will be encouraged.

22.13 Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.



Appendix A: **Norfolk Children's Services E-Safety Policy**

Please double-click on the icon to read the policy. This document complements Norfolk County Council's Code of Use and Code of Connection Policies.



Childrens_Services_E
-Safety_Policy.pdf



Appendix B: Password Policy

Purpose

This procedure is to define network passwords and their use. “The School” and “school” refers to Archbishop Sancroft Church of England VA High School.

Background

- a. Information stored on the computer desktop and the LAN (local area network) forms a part of the school’s valuable assets. Strong passwords promote a secure computing environment.
- b. To counter the forces of social engineering (this happens when an attacker tricks users into divulging passwords.) and brute force (these are attempts to gain unauthorised access to systems by trying every combination of letters and numbers until a match is found that allow access) methods of attack, we must be diligent in guarding access to our resources from internal and external threats by adopting strong passwords.
- c. Passwords are the primary authentication method for the school’s ICT resources and are currently the basic authentication method employed. Passwords ensure that only authorised individuals have access to specific computer systems and establish accountability for all changes made to system resources. Badly chosen passwords endanger the information that they are supposed to protect.
- d. The school needs to institute a robust password procedure if it is to move towards a single-sign-on environment. With a single-sign-on system, a user will be required to authenticate once to gain access to all network resources.

Scope.

This procedure applies to all staff and students, and any external contractors who are given computer accounts to access information systems owned by or operated by the school.

Responsibility

The staff in the Information Technology Department are responsible for the day to day operation of this procedure. Overall responsibility is with the Systems Engineer.

Applicable To

All Staff and Students

Description

Best practices.

1. Passwords should not be written down, emailed or spoken.
2. Passwords must be kept confidential and not shared with colleagues. This does not apply to generic departmental passwords, where a group manages the password.
3. Your username or variations of the username should not be embedded in your password.
4. Passwords must not be blank.
5. Passwords should not be typed or saved in electronic documents
6. Computer generated passwords must be changed following initial successful login.



7. Passwords must not be based on personal information (e.g. names of families, pets, name of your street, car registration numbers, telephone numbers)
8. Passwords must not be revealed to your line manager.
9. Passwords must not be revealed to anyone over the phone.
10. Passwords used within the school must not be used for external Internet accounts or online service providers.
11. Passwords must not be included in any automated login process.
12. Passwords must be unique from previous passwords. The previous passwords should not be re-used.
13. Complex passwords should be enforced for staff accounts only as students with learning difficulties may find these difficult to use.
14. Special arrangements for students with learning difficulties will be discussed between the ICT co-ordinator and SENCO.

Passwords must meet the following criteria:

1. Passwords must be at least six characters long.
2. Passwords must be composed of alphanumeric characters (alphabets – A..Z, a...z and numbers – base 10 digits – 0..9).
3. Passwords should include non-alphanumeric or special characters (e.g. !; £; \$;); (; %; &; *; #; @; ?; {; }; [;]; =; +; >; <; “;”).

Passwords must be strong.

Here are some methods for making strong passwords:

1. You can choose one or two lines from a poem or song and use the first letter of each word. For example ‘Always look on the bright side of life’ becomes alotbsol
2. Passwords are case sensitive: using the above example, the passwords alotbsol, Alotbsol and aLotBsol are different and the security of passwords can be increased if mixed case passwords are used.
3. One strategy for creating strong passwords is to replace letters with numbers or characters. For example Alotbsol becomes A10tbs01 where the letter “l” has been replaced with the digit “1” and the letter “o” has been replaced with the digit ‘0’.

Changing your password

Passwords must be changed under any one of the following circumstances:

1. At least every three months
2. Immediately, if a password has been compromised or after you suspect that a password has been compromised.
3. Passwords must be changed on direction from the ICT Department
4. Note: You should not change your password last thing on Friday or just before you go on holiday as you may forget it when you need to use it.



Good practice/handling

1. A number of shared local administrative passwords may be used on machines for specific departments and computer labs.
2. Passwords must be at least six characters long but preferably longer.
3. Passwords must be retired after three months.
4. Service accounts must not rely on admin accounts/passwords.
5. Accounts created for external contractors should be given restrictive rights to carry out their functions and the accounts should be disabled immediately following the completion of the appointed task.
6. Administrator/privilege passwords must not be disclosed to external contractors.
7. Default passwords that come with computer systems or services must be changed during installation or immediately after installation.
8. Passwords must be unique from all previous passwords. The last ten passwords must not be re-used.
9. All systems must wherever possible be set up to prompt the user to change passwords in fifteen days.
10. Critical systems must implement account lockout policies and be set up to disconnect idle sessions after a period of inactivity of thirty or 45 minutes.
11. Systems must be configured to enforce password changes.
12. The SNMP community strings must be changed from the standards defaults and should be different from the password used to interactively log in.
13. Privileged passwords should not be communicated via telephone fax or email.
14. A separate privileged account must be established for Norfolk CC ICT Solutions.
15. All administrative account passwords and defaults (e.g. SNMP strings, BIOS), wireless routers for all school equipment must be given to the Head Teacher for safe storage.



Appendix C: Backup Procedure

Purpose

This procedure is to ensure that the school has adequate and secure backups of all systems to enable a full recovery to be carried out in an emergency or a partial recovery on request

Scope.

This applies to all servers in use throughout the school by all academic and support staff.

Responsibility

Overall responsibility is with the Systems Engineer. A log should be kept on all backups made and test restores.

Definitions

Full System Backup is defined as a complete Tape copy of the system.

Description

There are 2 servers, which require backing up. Should a backup fail.

1. Access Veritas Backup Exec (or other software)
2. Ascertain by checking the logs why the backup tape did not eject
3. Inform the ICT co-ordinator & Head Teacher that the Backup has failed
4. Carry out any remedial action to rectify any faults

Schedule

A full system backup of each server should be made each Friday. However, incremental backups of changed data maybe made during the week. It is expected that if all the data for each server can fit onto a tape in the allotted time that a full system backup is made daily.

A full system backup might only occur only during periods when the school is in operation (term time & PD days).

The tape when ejected should be placed in a fire proof safe and a weekly backup stored in a fire proof safe in a separate school building (in another fire proof safe) or securely elsewhere according to the data security policy.

Week	Day	Tape Used
1	Monday	Monday
1	Tuesday	Tuesday
1	Wednesday	Wednesday
1	Thursday	Thursday
1	Friday	Friday 1
2	Monday	Monday
2	Tuesday	Tuesday
2	Wednesday	Wednesday
2	Thursday	Thursday
2	Friday	Friday 2
3	Monday	Monday
3	Tuesday	Tuesday
3	Wednesday	Wednesday
3	Thursday	Thursday
3	Friday	Friday 3
4	Monday	Monday
4	Tuesday	Tuesday
4	Wednesday	Wednesday
4	Thursday	Thursday
4	Friday	Friday 4 or Month

Tape cleaning

LTO tape drives– these require cleaning one a month or when the 'Use Cleaning Tape' light comes on.

System recovery

A test restore from backup is to be carried out on a monthly basis unless a recovery has occurred during that month.



Data Security

Backup Tapes are not to be removed from site without prior permission of the Head Teacher. Any tape removed from site by persons other than the Head Teacher must be approved by the Head Teacher and signed for. The Head Teacher may delegate this responsibility to the Systems Engineer.



Appendix D: Anti-Virus Procedure

Definitions

- a. Virus - A program that is designed to replicate
- b. Macro virus - A virus that lives inside word or excel documents
- c. Boot sector virus - A virus that lives on the boot sector of a floppy disk
- d. Partition sector virus - A virus that lives on one of the partition sectors on a hard disk
- e. File virus - A virus that lives inside an executable file (*.exe, *.com)
- f. Stealth - The level of visibility of the virus

Responsibility

The Systems Engineer is responsible for making sure the anti-virus is fully up to date and correctly configured on all machines. The ICT Co-ordinator will educate users about computer viruses.

Description

- a. All school workstations are to run the latest version of a virus protection programme. Currently this is provided by Norfolk ICT Solutions
- b. All users must be responsible for any infected files or media brought into the school
- c. If a Virus is discovered the infected computer **MUST** be switched off Immediately and the Systems Engineer informed
- d. File servers are to be scanned on a regular basis and any virus's removed.
- e. Users should be educated about computer viruses.
- f. Regular backups should be made of all file servers and critical workstations.
- g. Only software from reputable sources should be installed onto workstations and or file servers.
- h. File servers should run anti-virus software to stop any new viruses bypassing the workstation anti-virus software.
- i. Users should only have restricted access to file servers to minimise the spread of viruses across file servers.
- j. The Internet should not be trusted as a virus free source of files
- k. Updates of virus definition files should be hourly. Equipment where possible should have backup mechanisms to download updates.
- l. Workstation scanning to occur at least weekly, file servers daily during the night.
- m. Antivirus and security requirements must meet or exceed the policy of Norfolk CC and so the implementation of this policy may alter to increase the level of system security, especially in changing circumstances.
- n. The Systems Engineer will check against the list of all workstations and laptop connected to the network and make sure that each appears (where applicable) on the antivirus installation on the server.



o. All other OS's connected to the network (e.g. Linux, Macintosh) will have appropriate antivirus software installed and be monitored by the Systems Engineer.

p. Laptops/portable equipment should be configured to download updates via the network and also when they obtain an internet connection.

q. Systems Engineer will take immediate action when there is an issue regarding lack of antivirus software on a computer or the AV software is not updating.



Appendix E: **Staff Code of Conduct for ICT**

To ensure that members of staff are fully aware of their professional responsibilities when using information and communication systems equipment staff are asked to sign this code of conduct. Members of staff must read and understand the school's e-safety policy prior to signing.

I understand that the school ICT equipment and systems are the property of the school whether used on or off the premises.

I understand that it is a disciplinary offence to use any school ICT system or equipment for a purpose not permitted by its owner. Head Teacher will provide clarification if required.

I appreciate that ICT includes a wide range of systems, including mobile phones, PDA's, digital cameras; email and social networking. ICT use may also include personal ICT devices with the permission of the Head Teacher if used for school business.

I understand that school information systems and equipment may not be used for private purposes without permission from the Head Teacher.

I understand that my use of school information systems, Internet and email is monitored and recorded to ensure policy compliance.

I will respect system security and will comply with the Password Policy.

I will not install any software or hardware without permission.

I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.

I will respect copyright and intellectual property rights.

I will report any incidents of concern regarding the inappropriate use of ICT systems or equipment to the ICT Co-ordinator, e-safety co-ordinator, the Designated Child Protection Co-ordinator or Head Teacher.

I will ensure that all electronic communications that I make are compatible with my professional role. In addition I will obtain prior permission from either the Head Teacher or Finance Office (as appropriate) before a contract is made on behalf of the school via electronic means.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.



I have read, understood and accept the Staff Code of Conduct for ICT.

Signed: Capitals: Date:

Accepted for school: Capitals:



Appendix F: Laptop Agreement

Whilst using the school laptop you agree to follow the Schools E-Safety policy, including the Staff Code of Conduct for ICT.

The laptop is issued to you for you to carry out your professional duties. Monitoring software will be installed. Therefore you should be aware if you carry out any online banking, personal email etc. as these can be logged.

The laptop belongs to the school and must be returned to the school when you leave its employ or at the school's request. You may occasionally be asked to return the laptop to the Systems Engineer for software updates and upgrades.

The laptop should not be continually left at home; it should be brought to work every day. During term time you should connect the laptop to the network at least weekly in order to receive the latest updates.

The laptop is issued solely to yourself, do not pass it on to another member of staff. If you no longer require it, it must be returned to the Systems Engineer or Head Teacher. Whilst at home the laptop should not be used by other members of your household as you are responsible for the use of your laptop.

The laptop should not be used by students unless under direct supervision.

The laptop must not be left unattended in an insecure environment; particularly in cars overnight.

You must ensure that adequate insurance arrangements cover the intended use and location of the laptop. It is insured while at school and in your home, it is also insured in transit but only if you are travelling directly between the two. If you make any stops this will invalidate the insurance. If you will be using the laptop in a manner that is not covered by the insurance please contact the Finance Office to discuss extra insurance. If the laptop is damaged or lost in a situation where it is not covered by insurance, replacement or repair will not be funded by the school.

You are responsible for ensuring any additional software that is installed on this laptop is legally licensed (to the school) and may be asked to produce proof of this. If in doubt please consult the Systems Engineer or ICT co-ordinator.

You should not remove or install other antivirus, or install personal firewalls without permission from the Systems Engineer, ICT co-ordinator or Head Teacher.

You must ensure you are aware of any implications involved in storing confidential or sensitive data on the laptop if taking it off site.

You are responsible for any data that you place on the laptop. You are advised not to keep important data solely on the laptop. If the laptop develops software problems then it will be returned to the state in which it was issued, this will involve loss of data if you do not have it backed up.

Archbishop Sancroft High School ICT & E-Safety Policy



Laptop Name ?????? Serial Number ??????
Holder's Name ?????? Department ??????

I have read and understand the above

Signature

Date



Appendix H: **Sanctions for Student Misuse of ICT Network**

See next page



The following are Breaches of Network and Internet Protocol with consequences (in bold):
*the bans can be Internet and/or the network and might be lifted for planned curriculum activities with the normal class teacher

1. Allowing anybody to know your password for any reason.
2. Enabling anyone to access the network and/or the Internet as a user other than themselves, whether they are banned or not, under your user name and password.



3.	Attempting to access files or folders outside of my personal folder or student shared files.
a.	Parents notified by letter from ICT Co-ordinator & Head of Pastoral <u>AND</u>
b.	After school detention <u>AND</u>
c.	Up to a Two week ban *
4.	Using chat, network chat or messenger services on the network or the Internet.
5.	Accessing non-work related material including webmail. This does not include school webmail services.
a.	Parents notified by letter from ICT Co-ordinator & Head of Pastoral <u>AND</u>
b.	After school detention <u>AND</u>
c.	Up to a Two week ban*
6.	Gaining or attempting to gain access to the network and/or the Internet whilst banned.
a.	Parents notified by letter from ICT Co-ordinator & Head of Pastoral <u>AND</u>
b.	Two after school detentions <u>AND</u>
c.	Up to a month ban*
7.	Typing an unsuitable word into a search engine and/or typing an unsuitable URL (website address) into the address bar. ("Unsuitable" is defined as words/statements/material relating to computer based games (including consoles), material of a sexual nature, racism, obscene/swear words, items relating to non-conformist groups or groups of questionable origin/beliefs/political views when it not part of my curriculum work.)
8.	Having, placing or attempting to place unsuitable material: <ul style="list-style-type: none"> • On a floppy disc/CD/USB device or any other storage medium in school • Anywhere on the school network • On a laptop/palmtop or other electronic device in school including mobile phones/portable devices
9.	Pursuing or attempting to pursue unsuitable results from searches. Viewing or attempting to view or download any unsuitable results.
10.	Entering or attempting to enter a suspect site despite warnings from security software about unsuitable content.
11.	Sending/Downloading or attempting to send/download any unsuitable material in any electronic format.
12.	Trying to get around filtering services and other network security
13.	Conducting a business or making business transactions
14.	Attempting to access any other computer or networked device which they do not have permission to access.
15.	Attempting to install or executing any programs that they do not have permission to use.
16.	Repeat offences (1-6)
	Sanctions will be issued according to the specific nature of the breach and could include:
a.	Parents notified by telephone and letter from Senior Team <u>AND</u>
b.	Internal or External exclusion of at least one day <u>AND</u>
c.	Up to a Six week ban*



Appendix I: **Student AUP**
(document attached)

Title	Review interval	Last reviewed	Next review	Changes made
ASHS ICT and E-Safety Policy	1 year	20.10.09	October 2010	New policy