



## E Safety Policy and User Agreement

Section 1: Westborough High School E Safety Policy	Page 2
Section 2: Commitment to educating students in the safe use of ICT technology	Page 2
Section 3: School Commitment to ICT Security	Page 3
Section 4: School website and Photograph policy	Page 3
Section 5: Mobile phone technology	Page 4
Section 6: ICT – ALL USER AGREEMENT	Page 5
Requirements of all users	Page 5
School Rights	Page 6
Code of conduct for use of Electronic communication	Page 7
Protection for the school	Page 7
Protection for School Users	Page 8
Social Networking	Page 9
Monitoring and Interception	Page 10
Email Protocols	Page 10
Code of conduct for responsible use of the internet	Page 11
Cyber Bullying	Page 12
Appendix 1 - Copy of Letter for inappropriate use by students.	Page 13
Appendix 2 - Additional guidance for long term loan of school laptops	Page 14
Appendix 3 – Understanding passwords	Page 15
Appendix 4 - Consideration of Issues of Confidentiality and Security	Page 17

Appendix 5 - Additional Advice to Staff re Social Networking Sites	Page 18
Appendix 6 - E Safety Incident Log	Page 19

### **Section 1: Westborough High School - E Safety Policy**

The school has an e safety group comprising the designated Child Protection Officer, The governor responsible for safeguarding, The SLT Line manager, the Head of ICT and the Network Manager. The e-safety policy covers the responsible use of the school network and computers and also the safe use of the internet. A condensed version is applicable to students.

All users (including guest users) must sign the e safety policy agreement.

The policy will be reviewed annually and therefore will next be reviewed in September 2011.

The purpose of the school network, hardware and internet access is to raise educational standards, promote student achievement, support the professional work of staff and enhance the school's management information and administrative systems.

Users need to be aware that the misuse of telephones, E-mail and computers, could result in disciplinary action e.g. contravention of child protection procedures, the Computer Misuse Act 1990; or the Data Protection Act.

### **Section 2: Commitment to educating students in the safe use of ICT technology**

Students will use ICT and internet technology outside school so it is essential that we educate them so that they can evaluate risk and ensure their own safety and security.

Students will sign a usage agreement at the start of every year.

The curriculum will deliver training on the topics of ICT security, online crime, cyber bullying, child protection issues, virus management and protection, file management and backing up. This will be delivered in the main through the ICT curriculum, PSHE and citizenship although all subject areas are expected to encourage responsible use of ICT. The VLE will also be used to raise the profile of e safety.

Parents will be made aware of the e safety policy through the school website, prospectus and parent events.

### **Section 3: School Commitment to ICT Security**

Personal data will be recorded, processed, transferred and made available according to the data protection act 1998.

The school will ensure regular and robust methods are in place for backing up data and virus protection.

The school will take all reasonable precautions to prevent access to inappropriate material via our network. However, due to the scale of the internet, it is not possible to guarantee that unsuitable material will never appear on a school computer. The School and Kirklees Council cannot accept liability for the material accessed, or any consequences of internet access, particularly if accessed in violation of the rules laid out in this policy.

The content of the school website, network and VLE is the responsibility of the Assistant Head Systems and Strategy (P Monfort).

Complaints of internet or network misuse should be reported to the Assistant Head Systems and Strategy (P Monfort). The VLE has two link buttons for reporting misuse of ICT resources and also bullying.

Complaints of a child protection issue should be reported in accordance with the child protection procedures (L Tempest)

### **Section 4: School website and Photograph policy**

Contact details published on the school website will be the school address, telephone number, fax number and email address. No personal details will be published on the website.

Photographs that include students will be selected carefully and used in context. The following criteria for photographic use should be observed. Staff should:

- be clear about the purpose of the activity and about what will happen to the images when the activity is concluded
- be able to justify images of children in their possession
- avoid making images in one to one situations or which show a single child with no surrounding context.
- ensure the child/young person understands why the images are being taken and has agreed to the activity and that they are appropriately dressed.
- only use equipment provided or authorised by the organisation
- Students should not take pictures of staff or friends without their permission.
- report any concerns about any inappropriate or intrusive photographs found.

- always ensure they have parental permission to take and/or display photographs. At the start of the year all parents sign an agreement with the school which permits the school to use images of their child in a sensitive and appropriate manner. A list of parents who have not agreed to the use of their child's photograph for educational reasons is kept by Assistant Head Systems Strategy.
- not use images which may cause distress.
- not use mobile telephones to take images of children.
- not take images 'in secret', or taking images in situations that may be construed as being secretive.

Student full names will not be used anywhere on the website.

Parents will sign a home school agreement giving permission for photographs to be used. All users will sign the ICT user agreement extending permission for the use of photographs and video.

### **Section 5: Mobile phone technology**

Mobile phones can present both opportunities for learning as well as a distraction. The following protocols have been agreed and should be observed by staff and students.

#### **For students and Staff**

- Mobile phones are banned in school for students. Students caught with mobile phones on the school site will have the phones confiscated and returned at the end of each school term. Where students are required to bring mobile phones for a learning activity the member of staff making the request should provide written authorisation to the student.
- Staff should not use personal mobile phones to contact parents or students unless caller id is withheld. In any case, school communication facilities should be used where available.
- Staff should not use mobile phones in areas shared by students unless they are on duty outside the school building and an internal phone is not immediately available.
- Staffs are not entitled to examine the contents of a student's mobile phone unless they have the permission of the student. Where permission is not granted the school police officer should be contacted who has different rights to examine mobile phone content. In any case, where a student is suspected of committing an offence the Police should be involved at an early stage.
- Staff should not lend mobile phones to students since this may allow the student access to confidential contact details in the phone's address book.
- Staff should use school mobile phones on trips where students/parents might be required to contact staff.

## **Section 6: ICT - ALL USER AGREEMENT**

### **Code of conduct for responsible ICT use**

#### **Requirements of all users:**

1. The computer system at Westborough High School is owned by the school and is made available to students to further their education and to staff users to enhance their professional activities, including teaching. This Code of Conduct is to protect everyone, the students, the users and the school. It applies to all persons who use the school's systems.
2. Users will only use their own log-in and password. This includes technicians. Generic passwords and usernames will not be used or issued.
3. Users will not share passwords or logins.
4. Remote access to the MIS data by external companies is forbidden.
5. Users will ensure that unattended school laptops are secured (locked away), both on and off site. Laptops should be handled with care.
6. Users will not access other users' files, without the express permission of that person except where files are on shared areas.
7. Users will only use the computers for educational or Staff professional activities during lesson time.
8. Users should not use schools computers to play non educational games, internet based or otherwise.
9. Users must take all reasonable steps to ensure that material brought in from home are virus free.
10. Users are responsible for any School equipment taken off site for both its security and use whilst in their care. Where, for example, a digital or video camera is on loan users are responsible for removing all personal data.
11. Users accept that photographic images and videos of them taken in a school context may be used for public displays, the school website and intranet as well as for public media.
12. Users should not use School equipment, such as scanners, printers, digital cameras, video cameras for personal purposes where the school may incur an expense
13. User will not use external storage (USB pens, portable drives etc...) on school computers where they are uncertain as to the disk's origin and contents, and will only bring materials that are suitable for educational purposes onto site.
14. User must not undertake any activity that threatens the integrity of the school ICT system or that attacks or corrupts other systems.
15. User must respect the copyright of materials.

16. Users will not transfer sensitive data to removable media (USB pens, external drives, laptops) unless appropriate steps have been taken to ensure the data is secure and inaccessible to unauthorised users.
17. User must not use college computers or laptops for personal financial gain, gambling, political purposes or advertising.
18. Users must not install software onto the network/ office work stations or laptops without consent from the Network Manager.
19. Users must not use methods (hacking software) or sites (such as proxy servers) to bypass filtering and security systems.
20. Users should not store non school related files on school servers (e.g. software, games & music).
21. Student users are not permitted to use Staff laptops or workstations/ or accounts under any circumstances.
22. User will not display confidential information when using classroom projectors. Be careful when viewing files or emails, either switch off the projector or freeze the screen.
23. Limited use of facilities for personal use is acceptable in certain circumstances e.g. where it would be difficult to organise outside normal working hours. Such use must be restricted to lunchtime before/after school unless it cannot be avoided.
24. Social networking sites should not be accessed in school. Examples include facebook, bebo, twitter, msn messenger etc... unless specifically authorised as part of a planned lesson or work.
25. If users see anything on any school-owned computer that they are unhappy with or receive a message they do not like they must inform the Assistant Headteacher Systems and Strategy (P Monfort). This can be done directly or by using the links on the VLE for reporting ICT abuse or bullying.

### School Rights

26. Users should note that Westborough High School reserves the right to examine or delete any files that may be on its computer systems including emails. Where users have utilised pen drives or other memory devices they accept that they may also be examined by ICT staff. The school will also monitor the internet sites visited and all documents created and accessed. The school also reserves the right to deny access to any user who knowingly abuses the system and acts against this Code of Conduct, and where appropriate the school may invoke Disciplinary Procedures. Where a crime has been committed the police will be notified.

## Code of conduct for use of Electronic communication

27. Users should note that the school email system is provided to assist users in the performance of their jobs/study. It is also recognised that there may be occasions when users would wish to use the email system for personal reasons. This is permitted subject to the following considerations, which apply to all use of the email system, whether for business or private purposes. However, it is advisable and good practice to operate a separate email address (free ones are available on yahoo etc) for personal emails so that work/school and personal matters are kept distinct.

### Protection for the school

28. Users should note that all email sent or received will be logged and cannot be regarded as confidential.

29. Messages which may bring the school into disrepute or which a reasonable person would consider to be offensive or abusive must not be sent. Email messages are regarded in law as having the same status as words on paper; potentially libellous comments should therefore be avoided. Racist, sexist or otherwise offensive language is unacceptable.

The golden rule:

If you wouldn't say it in public or send it by <b>postcard</b> – don't e-mail it
--

30. The system may not be used for the exchange of messages concerning illegal activities.

31. The system may not be used for personal financial gain.


32. Use of the system by an individual should not have a noticeable effect on the availability of the system to other users.

33. Personal use of email and other computer systems should not be to the detriment of the individual's normal work activity.

34. Contractual commitments should not be made via email.

35. Internal school email, messaging or other internal materials should not be sent to destinations outside the school without the consent of the author and caution and consideration for the content should be exercised.
36. The forwarding of chain letters is strictly forbidden. This includes those purporting to be for charity or other good causes as well as those promising wealth or other personal gain. Virus warnings also come under the same exclusion – most of these are false and should only be forwarded to the ICT Team. Under no circumstances should these messages be forwarded to anyone else inside or outside the school.
37. Sending unsolicited messages of any kind to multiple internal or external destinations may be considered as “spamming”, which is an illegal activity in many countries, and is not permitted.
38. In all messages, users should remember that email is not a secure form of communication. Any messages that are sent will be passed over networks owned by other people. If the content of a message could cause problems for the school or cause financial loss should it become known, a more secure method should be used. (For example, send it by royal mail, speak face to face, send a password protected file and a password in a separate email).

#### Protection for School Users

39. The person logged into a workstation will be considered to be the author of any messages sent from that workstation. Users should always log out or lock their workstation when they are away from their desks. (press the windows key  and ‘L’ together). Under no circumstances should users send emails from a workstation which they have not personally logged into.
40. Users should not disclose their passwords to anyone else. It is also advisable to change passwords on a regular basis. (Press ctrl, alt & delete keys at the same time and select ‘change password’).
41. Users’ email addresses should not be disclosed unnecessarily. If users give their addresses when filling in surveys or other questionnaires they will be at risk of receiving unwanted junk messages. Other users’ email

addresses should not be disclosed without their prior consent.

42. Users should not subscribe to non-work related email lists. The volume of messages that can be generated is high and there is no control over the content, which may bring the user into conflict with the conditions outlined in this policy. (Use a personal email address for this).
43. Users should not open attachments to email messages unless they are expecting them or they have come from a trusted source. Under no circumstances should anyone run any .EXE.COM , .BAT files or open a .ZIP file from an unknown source without first contacting the ICT Technicians Team.
44. Email users should not use the email system to pass comment on confidential issues unless the text has been safeguarded as in para 11 above. (Users should delete emails with confidential information as soon as possible and save the file in a secure format).

### Social Networking

45. Users must not post negative comments on social networking sites referring to the school. Comments deemed to bring the school into disrepute, may be considered as 'gross misconduct' resulting in possible disciplinary procedures.
46. Users should never post personal details such as home or mobile phone numbers or private email addresses where other users can gain unauthorized access.
47. Users should not post information (text nor images) that may bring the reputation of the school into disrepute.
48. Don't put anything on your social networking sites that you would not want to see shared in the public domain.
49. Users are advised to set confidentiality parameters so that other non authorized users cannot see anything on the users profile other than the user's name and avatar (profile picture). Setting access rights like this is similar to being listed in a phone book. You can almost completely hide your self by using a pseudonym (nickname) so that other users cannot search for your profile. In this way users can ensure that other users only gain access to your profile by invitation.

## Monitoring and Interception

50. Users should note that the school reserves the right to monitor the use of its ICT systems to ensure that it remains within the law, to ensure compliance with its internal usage policies, and to ensure that the systems are operating efficiently.
51. Users should note that email traffic will be routinely monitored, including source and destination addresses, but not content.
52. Users should note that all emails will be checked for the presence of computer viruses. This checking will be carried out automatically and the content will not be accessed by any other user. Any emails found to be infected will be automatically deleted.
53. Users should note that in the event of their being unavailable for work due to illness or other reasons, and the information in the users email account is deemed necessary for job function to be carried out, then the mailbox will be opened to the individual's line manager. This will only be done with the authorisation from the Assistant Head Systems and Strategy or the Headteacher.

## Email Protocols

54. Users should observe the following email protocols.
  - a. Email is not a substitute for face to face or telephone discussion on personal or personnel issues. It is not advisable to put anything that is confidential or personal on email;
  - b. Messages should only be sent to those people for whom they are relevant;
  - c. The heading should clearly explain the subject of the message;
  - d. Messages should be as short and simple as possible;
  - e. The contents should be clear and unambiguous;
  - f. Action points should be in bold;
  - g. Any reply dates should be clearly stated;

- h. It is courteous to reply to all emails which ask for assistance or information. Not to do so means that the person seeking help has no idea whether the message has been acted upon;
- i. Only use urgent/priority status when the message really is urgent/priority.
- j. External letters received by email should be replied to in the same tone as the original. Just because the letter is emailed does not mean you can use the person's first name when you reply;
- k. Email letters should be filed in the same way as paper letters;
- l. In-boxes should be checked daily;
- m. Delete all unwanted "sent", "received" and "deleted" emails regularly;
- n. Do not open any unrecognised attachments, or any attachments from a sender you do not recognise. They may contain viruses that could damage the information on your machine and infect others. Just delete any such messages immediately.
- o. The following disclaimer should be added to all school e-mails and must be included in signatures: *"The views expressed in this message are personal and must not be considered to be the official views of Westborough High School"* To avoid having to type this out in every email you can add this text into your signature by selecting options in your emailing browser and adding the text into your signature box.

### **Code of conduct for Responsible use of the Internet**

- 53. The school internet access will be designed expressly for student use and include filtering appropriate to the age of the student.
- 54. User will only knowingly access sites and materials that are appropriate to work in a school.
- 55. Filtration by keyword and by web address will take place through the LA and also at the school portal. When access

is denied through filtration users can request that the web address be allowed.

56. When the filtration occurs at school level access can be allowed immediately where appropriate. Filtration at an LA level can also be removed by request but this process may take a number of days.
57. Accessing racist websites, websites encouraging discrimination, bullying or acts of violence and pornographic sites will be seen as an act of gross misconduct.
58. If users access the internet via their own personal connection they must ensure that any college files stored on the laptop are secure.
59. If users discover unsuitable sites the URL (address), time and content should be noted and reported to the network manager.

### Cyber bullying

60. Cyber bullying is the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else. While there is not a specific criminal offence called cyber bullying, activities can be criminal offences under a range of different laws, including:
  - a. The Protection from Harassment Act 1997
  - b. The Malicious Communications Act 1988,
  - c. Section 127 of the Communications Act 2003
  - d. Public Order Act 1986
  - e. The Defamation Acts of 1952 and 1996
61. Any user who is a victim of cyber bullying or witnesses another user being bullied is required to report the offence to the Assistant Head Systems and Strategy (P Monfort).

I have read, understood and agree with the ICT All user agreement.

Name: \_\_\_\_\_ Signed: \_\_\_\_\_ Date: \_\_\_\_\_

Headteacher: Signed: \_\_\_\_\_ Date: 05/05/2011

## Appendix 1

Dear

I regret to inform you that your child has been reported to me for inappropriate use of the school computer network. In this instance your child has

---

As a consequence your child has had their user rights cancelled for a short period of time. I would therefore urge you to discuss with your child the need for them to use the school network responsibly since inappropriate use can:

- waste school resources such as server memory,
- reduce internet bandwidth slowing the network down.
- cause other problems wasting the time of our technical support staff.
- detract from your child's learning opportunities.

In order for your child to be granted renewed access to the network I would ask you to sign and return the slip below via your child.

Yours sincerely

*P Monfort*

**P Monfort**

**Assistant Headteacher**

---

To be returned to the technicians office next to IT1.

Name: \_\_\_\_\_

Form: \_\_\_\_\_

I have discussed this matter with my child and they wish to resume normal access to the school network.

Parent Signature \_\_\_\_\_

I promise to use the network responsibly and agree to follow the policy on responsible use.

Student Signature \_\_\_\_\_

## Appendix 2

### **Additional guidance for long term loan of school laptops**

This protocol is designed to act as a guide for staff who have long term loan of a school laptop for use at home.

The ownership of the laptops rests with the school.

Staff who are provided with a laptop for use at home have full use of the laptop to support their work in school and also for personal use following the guidelines outlined in this document.

Staff are free to install software on the laptops providing all licence requirements are met.

Staff are free to choose their own Internet Service Provider and are responsible for any charges incurred.

Staff are reminded that they should not deliberately seek out pornographic, inappropriate or offensive materials on the internet and that they are subject to criminal legislation and disciplinary procedures for teaching and support staff should they do so.

Anti-virus software should be installed on the laptop and members of staff have the responsibility of keeping the software up-to-date and for scanning materials downloaded from the Internet.

Staff should always password protect important or sensitive school and pupil information.

It is their personal responsibility to ensure that back-up copies of such information are taken and held securely.

There are a number of legal requirements relating to the use of information and software (e.g. Data Protection Act, Copyright Act). Staff are responsible for understanding and complying with their legal requirements.

Staff should be aware that laptop computers should never be left in cars or in a place where an opportunist thief could take it. With most insurance companies laptops are covered in cars as long as they are not left unattended.

Staff should make sure that they are aware of the arrangements that have been made by the school for insurance cover on laptop computers and to follow any guidelines procedures established by the school to safeguard this cover.

If necessary staff should ensure that their home contents insurance covers the laptop whilst in their possession.  Staff are responsible for removing all personal data, documents and software from the laptop before it is returned to school.

Staff should sign a copy of this Laptop Protocol and return it to the Assistant Head Teacher Systems and Strategy.

Full name ..... post .....  
Signed ..... date .....  
Approved ..... date .....

## Appendix 3

### Understanding passwords

Wherever you use a password (such as logging on, setting a screen saver, encrypting or zipping files, securing the computer Administrator user account, etc) your security is only as good as your password and the measures you take to ensure that your password is not disclosed to unauthorised third parties. To be as secure as possible you should give careful thought to your password and make it as strong as possible by following the simple rules described below. You should never allow the computer to automatically save your password.

All passwords should:

- be at least 7 characters long - the most secure passwords are at least 14 characters long. Windows XP passwords can be up to 127 characters long. Increasingly, people are using *passphrases* rather than *passwords*.
- contain a combination of characters from the following groups :
  - letters A-Z, a-z (note : uppercase and lower case letters are different characters in most systems)
  - numerals 0-9
  - symbols ` ~ ! @ # \$ % ^ & \* ( ) \_ + - = { } | [ ] \ : " ; ' < > ? , . /
- have at least one symbol character somewhere in the middle
- be significantly different from prior passwords
- not contain your name, family names or user name
- not contain the birthday of you or your family
- not be a common word or name
- not contain anything else which is easily guessed (such as addresses and telephone numbers)
- not contain numbers substituting for letters (e.g. 1 for I, 3 for E, etc)

Password-guessing software uses one of three approaches: intelligent guessing, dictionary attacks, and brute force that tries every possible combination of characters. Given enough time, the brute force method can guess any password. However, it can still take years to guess a strong password. The best encryption systems are based on key generation and passwords can be whole sentences. These passwords can take millions of years for supercomputers to decipher.

### Caution

Before storing any copies of critical information in encrypted form, you should carefully consider the risks associated with losing or forgetting the passwords

because the data will be unrecoverable. Keep a record of the passwords you use and keep this record in **a secure place** (e.g. in the school safe).

If a keystroke monitor or other malicious code (such as a virus) is running on your computer, your password may be recorded when you type it. Automated virus checks protect against this but you should be vigilant of any devices attached to your machine and report anything suspicious or where your protection software does not appear to be functioning correctly.

## Appendix 4

### **Consideration of Issues of Confidentiality and Security**

All desktop, portable and mobile devices, including media, used to store and transmit personal information should be protected using approved encryption software.

Personal data held on laptop computers and portable storage devices (e.g. USB memory sticks) must be protected to prevent unauthorized access. It should not be kept for longer than is necessary for its intended purpose and it should be deleted after use or transferred to the network or CD/DVD and stored securely.

Protection can be provided in a number of ways.

For example :

- Laptops must have log in and password authentication
- Screen savers should be set with password protection and come on after a minimum of 5 minutes
- Password protection can be used on individual files or Zipped archives
- Encryption should be used where possible – on individual files, portable storage devices, or whole computers

Work at home must be carried out with similar consideration for security as office-based work. All staff working off the school site or at home must be aware of the additional and significant risks of :

information 'leakage' through being overlooked or overheard  
the opportunity for hacking presented by Bluetooth or Wi-Fi  
leaving sensitive school data accessible on home computer systems.

**Look after the security of school equipment and your own personal equipment. Make sure you:**

- Protect your computer using a screen saver password
- Install Antivirus Software
- install Antispyware Software
- Install a Firewall.
- Set up a secure wireless network at home.

## Appendix 5

### **Additional Advice to Staff re Social Networking Sites**

Don't be afraid to use social networking sites but protect yourself.

Don't allow students to be listed as friends on your social networking sites.

Be very wary of accepting ex students as friends on social networking sites. Remember they may have friends or family still in school who may gain access to your social networking sites.



**Flowchart for responding to E-Safety incidents in School.**

