

# **Staff Internet & Acceptable Usage Policy**



## **Acceptable Use Policy for the Internet and Electronic Mail by Wark C of E First School Staff**

## **1. Introduction.**

This document sets out the terms and conditions under which users will:

- Use technologies and devices in school, or in relation to school work
- Access the Internet
- Make use of resources / information on the Internet
- Disseminate information arising out of the Internet
- Disseminate information via the Internet
- Communicate using the Internet

This document applies to all staff, to whom the Internet is available via both networked and stand-alone computers within School with access to the Internet and also for home use of school lap tops.

## **2. Purpose**

The primary purpose of this document is to establish a set of rules and regulations to enable all users of the Internet to do so for the benefit of the school.

Additionally, this document aims to safeguard employees. Specifically to:

- Minimise (and where possible eliminate) the School's legal liability for the acts of employees using the Internet.
- Minimise (and where possible eliminate) the threat of damage to School property and or reputation by acts of employees using the Internet.
- Educate staff on their duties and obligations to the School and each other when using the Internet and the consequences of breaching them.
- Protect employees if this policy is breached by accident.

## **3. School Responsibilities**

### *Implementing this Policy*

The Headteacher and Board of Governors should implement this Policy in the way that best fits the working practices of the school. However, the implementation of this Policy should be carried out so that:

- Every user with Internet access is aware of it and understands its contents,
- Its regulations are enforced throughout the school,
- Breaches can be reported in a safe and confidential manner.

Under the authority of the Headteacher, the ICT co-ordinator will ensure that staff usage of devices, the Internet and electronic mail is carried out in accordance with this Policy. The ICT co-ordinator should also have control over who in the school has access to the Internet. This Policy must also form part of the induction programme and exit programme of all School employees who will have access to computers in the course of their work.

## 4. Warning against Deliberate Misuse of the Internet

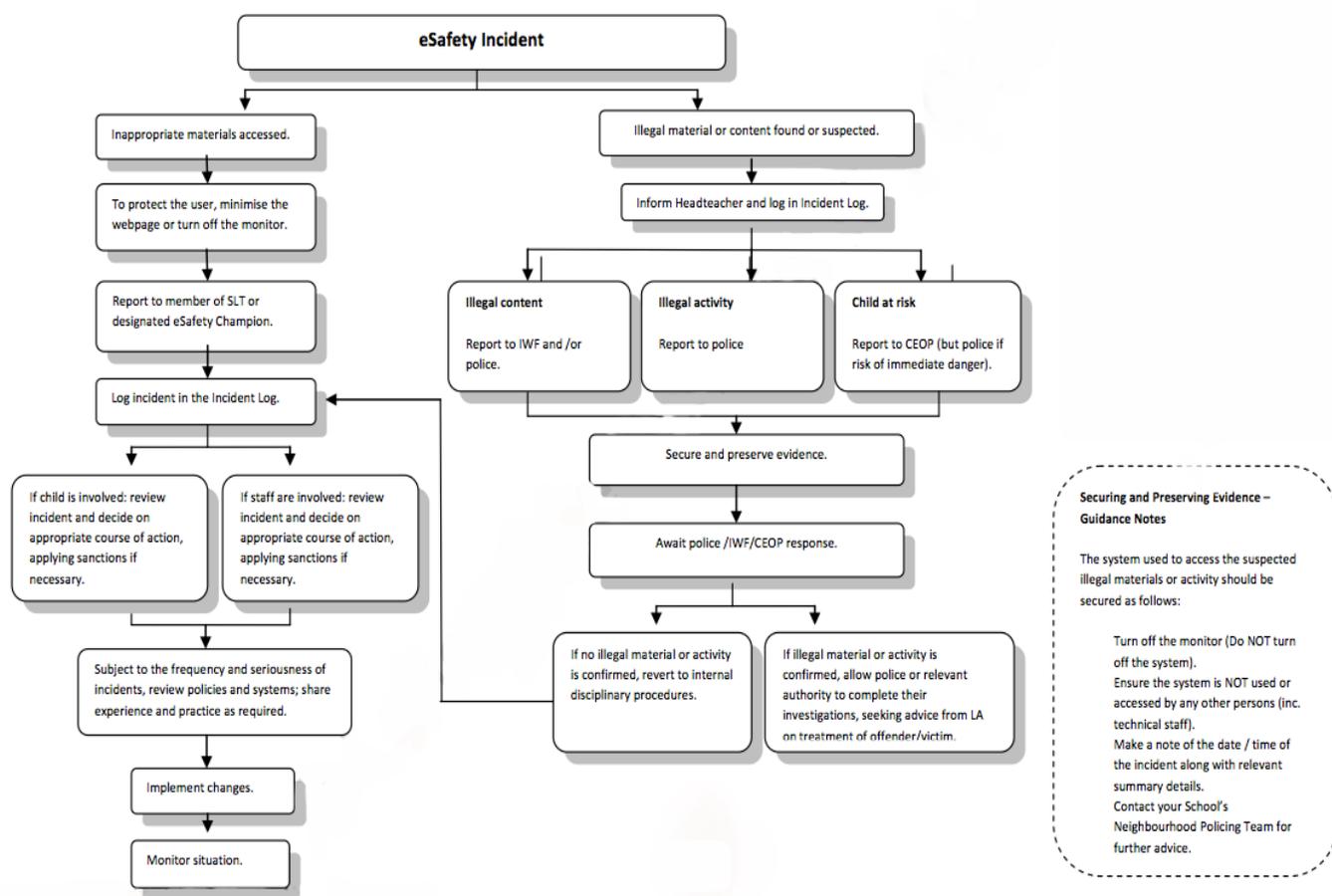
The Internet is a valuable resource. It also presents significant dangers to the School from staff who may choose to abuse it. Whilst each case will be judged on its own merits, the following warning is issued to all staff:

- (a). Any member of staff who commits a breach of any School Policy, regulation or Standing Order as a result of unauthorised use of the Internet (including electronic mail) will face disciplinary proceedings. Additionally:
- (b). If the School discovers that a member of staff has committed a criminal offence or has been party to the commission of one as a result of unauthorised use of the Internet, the Police will be contacted immediately,
- (c). The School will in no way indemnify a member of staff who has incurred any liability as a result of unauthorised use of the Internet. The School will seek financial redress from members of staff whose unauthorised use of the Internet causes the school to suffer a loss.

## 5. Protection of staff acting in good faith

It is fully recognised that a member of staff may accidentally breach this Policy whilst acting in good faith and in the course of their duties as a member of staff of the School. If a member of staff suspects this to be the case, they **MUST** notify the Headteacher and ICT co-ordinator **IMMEDIATELY** so that action can be taken to prevent or minimise damage and incidents can be logged.

The process followed where / when a concern is raised



## **6. Authorised Uses of the Internet using school property whilst on school premises.**

The school permits staff to use the Internet whilst in school in connection with school related matters only. This may include;

- The delivery of ICT lessons,
- Searching for lesson resources,
- Checking and responding to school e-mails using only school e-mail logins, and
- Other school related searches

Please note that users may be asked to justify accessing any site and internet usage is monitored by the ICT coordinator. A list of all websites accessed is viewed by the subject leader and details of staff who have accessed a site not obvious for school use will be passed on immediately to the Headteacher and investigated.

## **7. Unauthorised uses of the Internet**

Whilst an act that does not fit the above categories will be considered an unauthorised use of the Internet, user's attention is drawn to the following:

### *Strictly prohibited acts*

- The copying of software files from the internet should be kept to a minimum. No executable files should be copied from the internet. Software downloads must only be carried out by an ICT technician once permission has been sought. The technician will be responsible for ensuring that it is not faulty, is not infected with a virus and that all copyright requirements are met. If there is any doubt, the Head of ICT in North Tyneside should be contacted, via the School's nominated member of staff.
- Do not access any sites or download or print any files displaying material that the user knows to contravene the School's Equal Opportunities Policy. If such a site is accessed inadvertently, a manager should be informed immediately.
- Do not access any site that involves any form of gambling or betting,
- Do not access any sites which provide a discussion or "chat" forum which does not fit the authorised uses listed above,
- Do not access free or personal e-mail sites (e.g. Hotmail) in order to check private e-mail whilst on school premises or when logged onto the school or admin accounts provided on staff laptops,
- Do not order any goods via the Internet without consulting the Headteacher,
- Do not respond to surveys on the Internet on behalf of the School without consulting the Headteacher,
- Do not open a subscription account on the Internet on behalf of the School without express permission of the headteacher,
- Do not allow anyone other than an employee of the Council to use the Internet via the user's PC or school provided laptop.
- Do not use electronic mail for communication other than for purposes set out in Authorised Uses of the Internet, whilst on school premises or when logged onto the school or admin account on a school laptop,
- Do not leave PCs in a state where it would be possible for someone other than the normal user (or other legitimate user) to access the Internet. Staff are responsible for logging off or locking a PC when it is not in use.
- Do not leave your PC unattended without locking it to your login

- Do not let any other user access the Internet whilst on your logon.

It is the responsibility of all users to report any unauthorised acts as soon as it comes to their attention to the ICT co-ordinator, or Headteacher of the breach who in turn should investigate the breach in consultation with the Council's ICT Services Manager.

Additionally, users are requested to follow the principles of good practice set out below:

#### *Internet*

- Do not reveal your own (or any other person's) personal details eg. home address, telephone number over the Internet,
- Connection time on the Internet must be of the shortest possible duration.
- Keep a record of sites which may be of use to your school and inform your ICT coordinator or technician of them so that they can be added to a list of suitable sites for other members of staff to refer to.

#### *Electronic Mail*

- Electronic mail should only be used in the course of your work as a school employee and only using the authorised logins provided by the school/ Platform.
- You should only use your Northumberland e-mail account for all work related communications.
- Electronic mail is not a person-to-person communication, always use appropriate language.
- Never use electronic mail to send or forward chain letters or any material which may contravene School policies (e.g. jokes, pictures of a racist or sexist nature)
- Keep messages as brief as possible and related only to work issues.
- Only copy messages (i.e. cc or bcc) to people where it is of direct relevance.
- If you are attaching documents, always state the format (e.g. Word 97 or Excel 2000) of the file you are attaching in the body of the electronic mail message.
- At least once a week, ensure that all unwanted electronic mail messages are deleted from the Inbox, Sent and Deleted folders.
- Check your mailboxes regularly, at least once a day when in school.
- Ensure that messages arriving at your mailboxes are forwarded to another person if you are on leave for an extended period.

#### **8. Internet access on school laptops/iPads whilst not on school premises.**

- Your school laptop/iPad must be password protected for all accounts on the device.
- Staff may use the laptops/iPads for school related work only and not for personal use.
- You must not allow friends or family members to use your school laptop/iPad for any purpose.
- You must not access a home account whilst on school premises at any time and these may not be used to link up to any other software, including interactive whiteboards.
- You do not have the permission to download anything without seeking the permission of a LA technician or subject leader. If you are in doubt about what you may or may not access it is your responsibility to check before accessing. Laptops/iPads may be randomly collected in and checked by technician.

## **9. Use of Mobile Devices**

Example of devices:

Any USB device, MP3 players, Mobile Phones, Tablet devices

Wark C of E First School does not prohibit the use of mobile devices on the school network.

However, users should note the following items. These examples are for clarification. They are not exclusive.

Any mobile device must be checked for viruses and spam content before being attached to the school network.

Mobile devices must not be used to take photographs or sound clips of any person who is unaware of the action and who has not given their permission.

Any use of mobile technology to intimidate, bully, harass or threaten others will be counted as an infringement of network use. This may result in disconnection from the network or legal or civil disciplinary action. Uploading images and sound is only permissible if the subject involved gives permission.

Any images that involve children must not identify children by name and permission must have been agreed by the relevant parent / carer before posting. A record should be made of who will be taking the photos, why the photos are being taken, when they are being taken and what they are to be used for. This should all be documented in the risk assessment carried out before a school trip or event. The photos should then be stored in a safe area within the school LAN and only used for legitimate educational purposes as directed by the Headteacher.

## **10. Reviewing this Policy**

This Policy will be officially reviewed as the use of the Internet in the school develops although it may be that the policy must be changed before this time due to developments within the curriculum, school or local council. If you have any comments about this Policy, please pass them on to the school ICT co-ordinator.

## **11. School Implementation Details**

School Name: Wark CE First School

Date of Governors approval of this policy: July 2017

Nominated School member of staff for this Policy: Mike Boucetla

## **12. Member of Staff signature**

All staff must read the above policy and guidelines specified on the AUP form before access to the internet will be granted. They also have a responsibility to keep up to date with the School's acceptable use of the Internet policy and photographic images policy and accept that it forms part of their conditions of employment. Specific AUP guidelines have been designed for general staff, SEN staff and supply staff. These will be collected by the ICT administrator before login details will be given.

***This policy should be read in conjunction with:***

*Social networking Policy*

*Cameras and mobile phone usage*

*IT Security Policy*

*E-Safety Policy*

*Tapestry Policy*

# **Wark C of E First School Staff Information Systems Code of Conduct**

**To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.**

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I will not be involved with any online activities, either within or outside school that may bring the school, staff, pupils or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
- I understand that school information systems may NOT be used for private purposes whilst on school premises, e.g. accessing personal email accounts and personal internet use.
- I will use my Northumberland e-mail account for sending and receiving emails for work related purposes only and no other email accounts on school computers.
- I will only use the internet for work related purposes whilst at school or whilst logged into a school account using a school laptop.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will NOT disclose any passwords or security information to anyone other than an appropriate system manager.
- If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will ensure that my school laptop/iPad is password protected.
- I will ensure that no friends or family make use of my school laptop at any time.
- I will NOT download or install any software or hardware without prior permission.
- I will ensure that pupil's personal data is kept secure and is used professionally and appropriately in school. I will NOT take pupil's personal data off the school premises. Pupil's personal data will ONLY be stored on the schools server and NOT on laptops, memory sticks or any other portable device.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- Network access must be made only via the user's authorised account and password, which must NOT be given to any other person.
- I will NOT use chat rooms or any other form of social networking site.
- Use for personal financial gain, gambling, political purposes or advertising is NOT permitted.

The school may exercise its right to monitor and log the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of 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 agree with the Information Systems Code of Conduct.**

Signed: ..... Capitals: ..... Date:.....

# **Wark C of E First School Staff Information Systems Code of Conduct (Supply Staff)**

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I will not be involved with any online activities, either within or outside school that may bring the school, staff, pupils or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
- I understand that school information systems may NOT be used for private purposes, e.g. accessing personal email accounts and personal internet use.
- I will only use the internet for work related purposes.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will NOT disclose any passwords or security information to anyone other than an appropriate system manager.
- If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will NOT download or install any software or hardware without prior permission.
- I will ensure that pupil's personal data is kept secure and is used professionally and appropriately in school. I will NOT take pupil's personal data off the school premises. Pupil's personal data will ONLY be stored on the schools server and NOT on laptops, memory sticks or any other portable device.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- Network access must be made only via the user's authorised account and password, which must NOT be given to any other person.
- I will NOT use chat rooms or any other form of social networking site.
- Use for personal financial gain, gambling, political purposes or advertising is NOT permitted.

The school may exercise its right to monitor and log the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of 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 agree with the Information Systems Code of Conduct.**

Signed: ..... Capitals: ..... Date:.....