STOKE park in partnership with students and parents

E-Safety Policy

Last Reviewed September 2014

Introduction

It is our duty and responsibility to provide a safe and secure learning environment for the entire school community, which includes safe and appropriate use of information and communications technology.

Purpose

Through this policy statement, Stoke Park School seeks to create a learning environment in which all feel safe, and yet which actively promotes the use of electronic communication, internet, digital and wireless technologies.

Principles/Scope

We recognise that use of ICT provides a vast opportunity for students to learn, promotes creativity, stimulates awareness and enhances learning. However, this requires us to educate students about the benefits and risks of using these technologies, and to provide safeguards and awareness for users to enable them to control their on-line experiences.

We are committed to ensuring that use of ICT :

- raises educational standards and promotes student achievement
- develops the curriculum and makes learning exciting and purposeful
- enables students to gain access to a wide span of knowledge in a way that ensures their safety and security
- educates students in the safe use of ICT
- enhances and enriches the lives of our students.

Procedures

Curriculum : through delivery of the curriculum in ICT, PSHE and other related subject areas, we will ensure that the students are given appropriate advice and guidance with regard to ensuring their own safety whilst using ICT. This will also be reinforced through specific events such as assemblies and tutor/pastoral time.

Network Security : the school's ICT Support Team will ensure that effective safeguards and filters are in place to minimise the risk of students accessing data or websites which are inappropriate. However, students and staff also have a duty to advise the ICT Support Team if they see any inappropriate material, so that such sites can be added to the school's "banned" list. Use of ICT will be monitored by staff and through use of software packages to ensure that appropriate use is being made of the equipment and software made available.

Internet Permission Forms : before students are issued with passwords, parents/carers will be asked to read and sign a permission form for their child. This includes guidance to the parent/carer on how they can also help their child to use ICT safely. (Form included with this guidance, as Appendix 1.)

Individuals' use of ICT : the school expects all staff and students to use the internet, mobile and digital technologies responsibly, and strictly in accordance with the following conditions :

- users shall not visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments which contain or relate to :
    - indecent images of children ○ promoting discrimination of any kind ○ promoting racial or religious hatred ○ promoting illegal acts
    - any other information which may be offensive to peers or colleagues, such as abusive images, promotion of violence, gambling, criminally racist or religious hatred material, or other such material which could cause offence

- in addition to the above points, users shall not undertake activities with any of the following characteristics :

- corrupting or destroying other users' data ○ violating the privacy of others ○ disrupting the work of others
- using the network in such a way as to deny the service to other users (such as deliberately or recklessly overloading access links or switching equipment)
- misuse of the network, such as introduction of viruses, or use of software which bypasses internal security measures
- using services in any way to intimidate, threaten or cause harm to others

- users will be expected to report, immediately, any inappropriate material found through internet or other ICT usage

- there is a clear expectation (and indeed a governing body/school directive) that any communication which could be deemed to be "of a personal nature" will not be permitted between the distinct groups of staff and students (including 6th form students). This includes membership of "face-book" groups or similar; this school has determined that it is inappropriate for staff and students to be linked as "friends". Professional communication relating to school work is, of course, acceptable.

  Staff will sign the pro forma at Appendix 2 to confirm their understanding of this requirement, and to acknowledge receipt of, and adherence to, the school's adopted "Acceptable Use of ICT Facilities Policy". Guidance for staff on appropriate use of ICT and internet is attached as Appendix 3.

Failure to observe the school's expectations and conditions of use will be considered a serious breach of the school's safeguarding and equalities practices, and as such will result in appropriate action being taken through the school's behaviour policy (for children) and the school's disciplinary procedure (for staff); this could include formal reporting to the Police where necessary. It may also be necessary for the school's Child Protection Officer to become involved in specific instances, and this involvement may be reported to the Local Authority, Social Services and the Police as required.

Policy Review

The policy will be reviewed at regular intervals (at least annually) with the School's Governing Body to ensure that it remains accurate, and that individuals are kept aware of their responsibilities.

Accessibility

This policy statement is available on request from the school, and will be available via the school's web site. The format of the plan can be adapted as required (e.g. large print, language other than English).

Feedback on this policy is welcomed – please send any comments via the School's main Reception Office.

APPENDIX 1

Parent Permission Form - Use of the Internet

Please complete and return this form to Reception

Safety when using the Internet :

We want the children to use the Internet safely. We will give advice and instruction to the children in this respect, but please would you also discuss the following points with your child before signing the form :

- Help your child to understand that they should never give out personal details to online friends they do not know offline
- Explain to your child what information about them is personal, such as e-mail address, mobile number, school name, sports club, arrangements for meeting up with friends, pictures or videos of themselves, their friends or family. Small pieces of information can easily be pieced together to form a comprehensive insight into their lives and daily activities
- Make your child aware that they need to think carefully about the information and pictures they post on their profiles. Inform them that once published online, anyone can change or share these images of them
- It can be easy to forget that the internet is not a private space, and as result sometimes young people engage in risky behaviour online. Advise your children not to post any pictures, videos or information on their profiles, or in chat rooms, that they would not want a parent or carer to see
- If your child receives spam or junk email and texts, remind them never to believe their contents, reply to them or use them
- It's not a good idea for your child to open files that are from people they don't know. They won't know what they contain—it could be a virus, or worse - an inappropriate image or film
- Help your child to understand that some people lie online and that therefore it's better to keep online mates online. They should never meet up with any strangers without an adult they trust
- Always keep communication open for a child to know that it's never too late to tell someone if something makes them feel uncomfortable

(extract taken from guidance provided by CEOP - Child Exploitation and Online Protection)

Giving Permission :

PARENT

I agree/do not agree* to my child _____having Internet access.
*(*please delete as appropriate)*

As the parent/carer of the student signing below, I grant permission for my child to use e-mail and the Internet.
I understand that students will be held accountable for their own actions. I also understand that some materials on the Internet may be objectionable, and I accept shared responsibility with the school for setting standards for my child to follow when selecting, sharing and exploring information and media.

Signed _____ (parent/carer) Date _____ Home Tel No _____

STUDENT

As a school user of the Internet, I agree to comply with the school's rules on its use. I will use the network in a responsible way, observe all the restrictions explained to me by the school **and will report any unsuitable material I may find**.

Signed _____ (student) Tutor Group _____ Date _____

APPENDIX 2

Staff Acceptance Form - E-Safety Policy and Use of ICT

Please complete and return this form to the School's Business Manager

Name : _____

- In signing below, I confirm that I have received and read the school's E-Safety Policy
- I undertake to comply with the requirements of the Policy and understand that if I am in breach of those requirements and directives, the school's disciplinary process will be invoked
- I understand that any concerns about access could be raised with the School's Child Protection Officer, and/or with the Local Authority, Social Services and the Police.

Signature : _____

Date : _____

APPENDIX 3

Acceptable Use of ICT Facilities Policy

1.0 POLICY STATEMENT

1.1 Coventry City Council supports the appropriate use of Information and Communications Technology facilities (including telephones, Internet, email and related services) that are provided for our employees and other authorised users.

This policy provides guidance about acceptable use, for the purpose of:

- sending or receiving email messages and attachments
- the use of the Internet for browsing and downloading information
- the use of telephones.

The purpose of implementing an ICT usage policy is to ensure that people understand the way in which these systems should be used in the working environment and to enable employees, other users and the organisation to gain the maximum value from technology. The policy describes the standards that users are expected to observe when using these facilities. It also ensures that employees and other users are aware of the consequences to themselves or the organisation (ie disciplinary action, putting the organisation at technical or commercial risk) should the technology be misused.

2.0 SCOPE & APPLICATION

2.1 The principles of this policy apply to:-

- All employees of the City Council and Elected Members,
- Employees and agents of other organisations who directly or indirectly support or use Coventry City Council IT systems including:-
- People and organisations we have contracted to work for us
- Outside organisations working in partnership with us
- Volunteers, students or any other authorised people working with or for us

2.2 Human Resources Service in conjunction with the Finance & ICT Directorate's Information Governance Team maintains the Policy. It is a condition of use of ICT facilities that the user agrees to be bound by the relevant Council policies and procedure.

2.3 The policy establishes a framework within which users of the facilities can apply self-regulation to their use. It is designed to advise users that their usage will be monitored and recorded. This policy should be read in conjunction with the **Corporate IT Security Policy**. It also links to a number of other policies and regulations in particular the **Employee Code of Conduct**, the **Equality Strategy**, the **Guidance for Managing Grievances of Harassment, Victimisation and Discrimination,** and the **Disciplinary Procedure**.

2.4 This policy contains important rules covering the use of ICT facilities. IT and Telecommunications security is viewed seriously by the Council. It should be remembered that use of ICT facilities in an unacceptable or inappropriate manner and breach of this policy may lead to disciplinary action or other action appropriate to the users status being taken. This action will also apply to those who knowingly permit, or enable, through failure to apply the IT Security policy, abuse to take place, (e.g. the sharing of passwords to obtain IT access). If users are in any doubt about what constitutes acceptable and appropriate use they should contact their line manager, HR (in the case of employees) or relevant City Council contact who enabled the provision of the IT facilities, or the IT Security Team.

Coventry City Council may respond to breaches of the policy by:-

- Giving an informal warning
- Restricting access to the Internet/email facility
- Withdrawing the facility completely
- Taking disciplinary action (in the case of employees). (Disciplinary action will be carried out in accordance with Coventry City Council's disciplinary procedure which is available to view on the Intranet or from the Directorate HR team)
- Taking action appropriate to the status of the authorised user
- Giving information to the police for possible criminal proceedings.

2.5 To comply with the Human Rights Act (1998) and the Regulation of Investigatory Powers Act (2000) employees should note that the use of Council ICT facilities will be monitored by specialist software. This is to maintain the effective operation of the Council's systems, and to comply with the Corporate IT Security Policy. Managers will be notified of any non-compliance issues. All inbound/outbound email will be monitored for attachments, and email may be inspected to ensure compliance with the Corporate Information and IT Security Policy. Internet usage including the level of usage and sites accessed will be monitored. Telephone usage will also be monitored.

Reporting of suspected or actual breaches of policy may also occur from proactive audits and day-to-day technical administration activities.

Monitoring arrangements will operate on a continuing basis and will be proportionate to the impact on the Council in accordance with relevant legislation. The purpose of monitoring will be:

- Investigating or detecting unauthorised use of ICT facilities, including the prevention of crime
- Determining if communications are relevant to the Council's business
- Demonstrating standards that should be operating.

By accepting the conditions that are laid out in the "pop-up" on the users screen, the user will be deemed to have given their consent for Coventry City Council to monitor ICT facility usage. Employees in particular are reasonably expected to give this consent as part of their contract of employment to enable them to undertake their duties.

Employees Acceptance of terms

I confirm that I have read the ICT usage policy. I fully accept the terms & conditions of use in relation to the monitoring of my use of the Council's ICT facilities, including Internet usage and the interception of Emails where provided for by the policy.

OK

3.0 Personal Use

3.1 The main purpose for the provision of ICT facilities by the City Council is for use in connection with the approved business activities of the Council. The City Council permits the use of its ICT facilities by employees and other authorised users subject to the following limitations:

3.2 The level of usage will not be detrimental to the main purpose for which it is provided, i.e. Council business, and priority will be given to the use of resources for this main purpose.

3.3 Personal use must not be of a commercial or profit-making nature or for any other form of personal financial gain and must not be of a nature that competes with the Council's business or results in unauthorised expenditure to the Council, eg excessive printing.

3.4 Personal use must not be connected with any use or application that conflicts with an employee's obligations to the Council, as their employer, or with any of the Council's policies or procedures and must comply with all such policies and procedures.

3.5 The Council recognises that employees occasionally need to deal with domestic and family needs during working hours. Employees may use office telephones, business mobiles (and similar devices) or email for such purposes providing the level of usage does not affect their level of performance or conflict with Council business.

3.6 The policy is to enable employees to manage <u>essential</u> family and domestic issues and is not to enable employees to maintain social contacts during working hours e.g. on-line social chatting. The private use of Council facilities should be kept to a minimum. This also applies to incoming calls.

3.7 Personal calls to premium rate lines are unacceptable.

3.8 Personal international calls should only be made if the employee is travelling abroad for work commitments and any such calls should be kept to a minimum.

3.9 Employees are permitted to carry out a maximum of two hours non-work related ICT usage per week, outside of their normal working hours. (This may be before or after work or during lunch breaks.) This may be a combination of Internet, email, phone, printing or other application usage. Employees wishing to use the Internet for study supported by the organisation should discuss the matter with their line manager. Such usage will be excluded from the two hour per week limit

3.10 Extended personal conversations via telephone or email, use of chat rooms and non-work related Internet browsing will not be permitted within working hours.

3.11 Employees will be allowed a maximum of 10Mb for the storage of "non-work" information. Personal files should be stored in the "my documents" folder which should be regularly checked and files deleted.

3.12 Where an employee's level of performance is affected by unreasonable personal use of the Council's ICT facilities or where abuse of the Council's facilities is identified, disciplinary action may be taken and repayment of call costs may be required. Line managers are responsible for promoting good practice and ensuring that employees are aware of this policy.

4.0 Legislation

4.1 The City Council and its employees must comply with all legislation affecting the use of ICT facilities. For further information and guidance on these Acts please refer to Appendix 1 of the Corporate Information & IT Security Policy.

4.2 The Council is committed to equal opportunities and this is demonstrated through its' Equality Strategy and associated policies. These policies reflect current legislation in this area. The Council will not tolerate discrimination, victimisation or harassment and in particular the use of ICT facilities for such acts.

4.3 Under the Data Protection Act 1998, you should only obtain, send or store relevant and accurate information about individuals in accordance with the registered purposes for holding same. Individuals have a right to see what information is kept about them, including emails. Information and guidance about the Data Protection Act (UK) 1998 is available from your Directorate's Data Protection Information Governance Lead Officer. Their role is to provide local data protection advice and training on the Data Protection Act. If you are unsure who your representative is please refer to the list of Information Governance Lead Officers, which is available on the Intranet.

4.4 The Computer Misuse Act 1990 applies to everyone who uses a computer and means that people who commit some form of computer crime may be punished in the criminal courts. The Act recognises as offences such activities as hacking, electronic eavesdropping and the deliberate dissemination of viruses, code or "malware".

5.0 Installation of Software

5.1 For the protection of employees, Coventry City Councils Corporate Information & IT Security policy prohibits employees from installing software onto their PC's. This includes software that could be downloaded, installed or run from the Internet, for example files that have a name ending in .exe or .com, as these may introduce viruses or code to the system. Where software is required for service delivery prior authorisation must be sought from your line manager. **(Reference Section 5.5b of the Corporate Information & IT Security Policy).**

In exceptional circumstances, non Serco staff can load software, but prior to installing it agreement must be sought from Serco, Desktop Delivery Team, Line Manager and any other relevant organisation.

6.0 Use of Email

6.1 Email facilities, as with all other IT facilities provided by the Council, must be used mainly for the business of the Council. Storage of emails and/or attachments on the servers takes up space on the server, which the City Council has to pay for. Users are reminded that storage of personal emails must be kept to a minimum, and in line with Sections 3.11 and 6.3 of this policy.

The storage of large personal documents or emails (especially when they contain photos, movie, music files etc) on the email or the Storage Area Network (SAN) servers causes unnecessary expense to the Council by requiring us to purchase additional storage space.

Users should therefore ensure that:

- business emails stored on the server contain text only
- business required attachments should be stored on the SAN

- personal emails and other documents should be stored locally under "My Documents". Such storage must not exceed 10MB
- regular housekeeping of business and personal emails and other attachments must be undertaken.

6.2 The use of Coventry City Council's email system to solicit trade, or to advertise services for private commercial purposes, or the unauthorised advertising of goods and services is strictly forbidden. This applies equally to current and former employees. Unsolicited "junk" mail or "spam" must not be sent by email.

6.3 Large file attachments (in excess of 10mb) including large graphics files (such as .jpgs or multimedia .mpgs) should not be moved by general email or stored on the server. This is to ensure that proper capacity planning can take place on the network. In the event of a problem ring the IT Help Desk (Serco extension 4040 or 0845 4589193).

6.4 Email is a powerful and useful business tool, however messages sent in this way are documents of the Council and the content and tone of messages should reflect this fact. Laws over libel, defamation, discrimination etc apply to the content of emails as for any other written matter. All employees are therefore responsible for maintaining the Council's public image and no abusive, discriminatory, harassing, inflammatory, profane, pornographic or offensive language or other materials are to be transmitted through the Councils' systems. Extreme care must be taken when writing messages, both in the content of the message and its circulation. Be aware that email is not generally considered to be "secure". (See Section 6.7 for encryption facilities). Only send messages that you would be happy to have publicly quoted, or that you would be happy to read out in Court. The Council will use appropriate disclaimers to provide the necessary legal protection.

6.5 You must not access another user's email system without their permission, and this should be granted via 'email permissions'. The facility to grant email "permissions' is available in Outlook and it allows you to define the level of access a colleague may have to your email account (eg read only of your Inbox), thus removing the need to disclose your password and ID. All line managers should have "permission" to view relevant folders in the event of absence due to holiday or sick leave. The guidance notes for this are available in Outlook Help. The sharing of IDs and passwords is not permitted.

Similarly, business related documents that may be required by colleagues should be appropriately stored on the SAN to allow access.

6.6 You must not send unsolicited, irrelevant or inappropriate email to news groups or mailing lists on the Internet.

6.7 External email is susceptible to interception. Emails containing sensitive or confidential information should be sent in encrypted format. If you require this functionality contact the Corporate IT Security Team.

6.8 You must not use email as a mechanism to introduce unauthorised software.

7.0 Use of Internet

7.1 You should not use Council Internet accounts for any of the following purposes:-

(i) Breaking through security controls, whether on our equipment or on any other Computer System.
(ii) Accessing Internet communications (such as emails) that are not intended for you (even if not protected by security controls) or doing anything which would harm the ability of others to access Internet resources that they are entitled to access.
(iii) Deliberately accessing or sending computer viruses or similar software.
(iv) Deliberately sending, accessing or creating material which is obscene, sexually explicit, pornographic, racist, defamatory, (harms someone's reputation), hateful, encourages or shows violence, describes techniques for criminal or terrorist acts or otherwise represents values which are against those of the Council as represented by its strategies, policies and procedures.
(v) Knowingly doing anything that is illegal.
(vi) Political campaigning or private business.
(vii) Any activities that could cause damage or disrupt networks and systems.

7.2 The Internet can provide high-level information, very quickly, however search activities should be focused and work related. Excessive search activity may constitute time wasting and will be addressed through normal Council procedures.

7.3 Different access and service levels may be given to employees, depending on the nature of their work. Access to restricted or normally prohibited sites may be given to specific employees, if the nature of their work demands it. Applications for this should be made to the Corporate I.T Security Officer. The City Council reserves the right to monitor Internet usage and to block access to certain Internet sites if it becomes necessary.

7.4 To comply with copyright legislation and to protect the assets of the Council, employees are not permitted to download any programs from the Internet and install them. Refer to Section 5.1 of this policy and 5.5b of the **Corporate Information & IT Security Policy**. You should not copy information that other people have created and re-send it without permission from (or at the very least acknowledgement of) where it originally came from, even if the content has changed.

8.0 Use of Telephones

8.1 Employees have a responsibility to ensure that telephone access, provided to them to enable them to carry out their duties, is not abused. The City Council will undertake periodic monitoring of the use of telephone facilities.

8.2 Employees who are required to use a mobile, or similar devices (e.g. Blackberry) for business purposes will be required to declare all private calls and make payment for them. This will include the VAT elements of the call.

8.3 The City Council recognises that from time to time employees make business telephone calls on their personal mobile phones. The use of an employee's personal mobile phone should be kept to a minimum and where at all possible landlines used. The City Council will expect to reimburse the employee for any business calls made on personal mobile telephones. The reimbursement will be the call charge plus VAT. (Where free minutes are used the amount reimbursed will be equivalent to that had there been a charge attached to the call). Employees should keep a record of any business calls and the reason for the call if they wish to be reimbursed.

8.4 Managers should not expect employees to utilise their personal phones on a regular basis. Should the need for a mobile phone for business use be identified then appropriate arrangements should be made through the Council's corporate contract. Particular attention should be made to the need for risk assessment where the need for a mobile phone is identified for reasons of safety.

8.5 Where use of home telephones and mobile telephones are part of an employee's job, their use and any payments relating to them will be specified as part of the contract. Managers should arrange for Directorate HR teams to be informed if this becomes the case during the course of employment.

8.6 Council telecommunications equipment may be used for essential family and domestic issues providing such use is not excessive and does not conflict with Council business or policy.

Such equipment should not be used for maintaining social contact during working hours.

8.7 Line Managers have a responsibility to monitor usage and to promote best practice

Email & Internet Usage FAQ's

1.	Can I use email /the Internet/ Microsoft applications and telephones for personal use?	Yes, outside of working hours and subject to the provisions outlined in this policy.
2.	How will my emails be monitored or filtered?	The email system will be monitored by the IT Security Team using M@ilMeter software. Reports on usage in directorates will be sent to HR managers for discussion with Management Teams. Filtering software is used to reduce the impact of junk mail (aka spam) and access to inappropriate Internet sites Attachments to emails will also be monitored by the Information Security Team to identify images which are unacceptable for transmission across the organisation.

3.	Will my emails be private?	No, email by its very nature is not secure. The City Council has a right (with the employee's consent) to intercept or inspect emails to ensure compliance with all other policies. All employees will have consented to the monitoring (in accordance with the terms of the policy), by way of the "pop – up" that will appear on users screens, prior to access being granted and/or via the terms and conditions of employment
4.	Can I forward jokes/pictures to colleagues?	No, the Council's facilities are provided for the main purpose of the business of the Council, ie delivering services to the public. All employees are responsible for maintaining the Council's public image and no abusive, discriminatory, profane, harassing, inflammatory, pornographic or offensive language or other materials are to be transmitted through the Councils' systems. Extreme care must be taken when writing messages, both in the content of the message and its circulation. (See section 6.4) Even jokes/pictures that you believe are lighthearted may cause offence.

5	What do I do if people are sending me unacceptable emails or "spam"?	You should inform your line manager immediately, and the IT Security Team who can then block the sender. Further information on "Spam" is available on the Intranet.
5.	How will my Internet use be monitored?	All Coventry City Council pc's and other devices that deliver ICT facilities will be subject to specialist monitoring software to ensure the safety of employees and to provide compliance with all existing policies. Random sampling of websites accessed will be undertaken and website access will be monitored where disciplinary investigations are undertaken. (See Section 2.5).
6.	Which Websites are prohibited?	All Websites that are pornographic or sexually explicit, violent, racist, obscene, promotes terrorism, illegal or otherwise unacceptable. Filtering software will be employed to exclude as many of these sites as possible.
7.	What if I accidentally access a prohibited site?	Explain to your line manager as soon as you can, and let the Information Security Team know so they can block the site.
8.	Can I use the Internet to purchase items for personal use (eg holidays, insurance books etc)?	Yes, provided you are not acting as a representative of Coventry City Council, and it is outside your working hours. The City Council can take no responsibility for the misuse of personal details or debit/credit cards when the Internet or email is used for these purposes.
9.	How will my telephone usage be monitored?	Managers are responsible for monitoring usage and are provided with reports.
10.	What is my responsibility as a manager over access to ICT facilities?	You must ensure employees are aware of, and comply with, the policy. Ensure your employees are aware of the monitoring software in place, and that they are courteous and professional in their communications. If you have concerns relating to an individuals level of usage of ICT facilities discuss these with your Directorate HR team.

11.	Can I have a photo of my dog/car/baby as a screensaver?	Yes, you can have a personal photo as a screensaver, or "wallpaper", provided it takes up no more than 10 MB of memory, and complies with all other Council policies, i.e. it must not cause offence.
12.	How do I know if I'm near my 10MB storage limit?	The storage limit can be accessed when viewing a folder contents in Windows 2000. The size of the folder is given at the bottom of the screen, e.g. 4.41MB
13.	How can I contact the Corporate IT Security Team?	You can contact the IT Security Team at ITSecurity@coventry.gov.uk