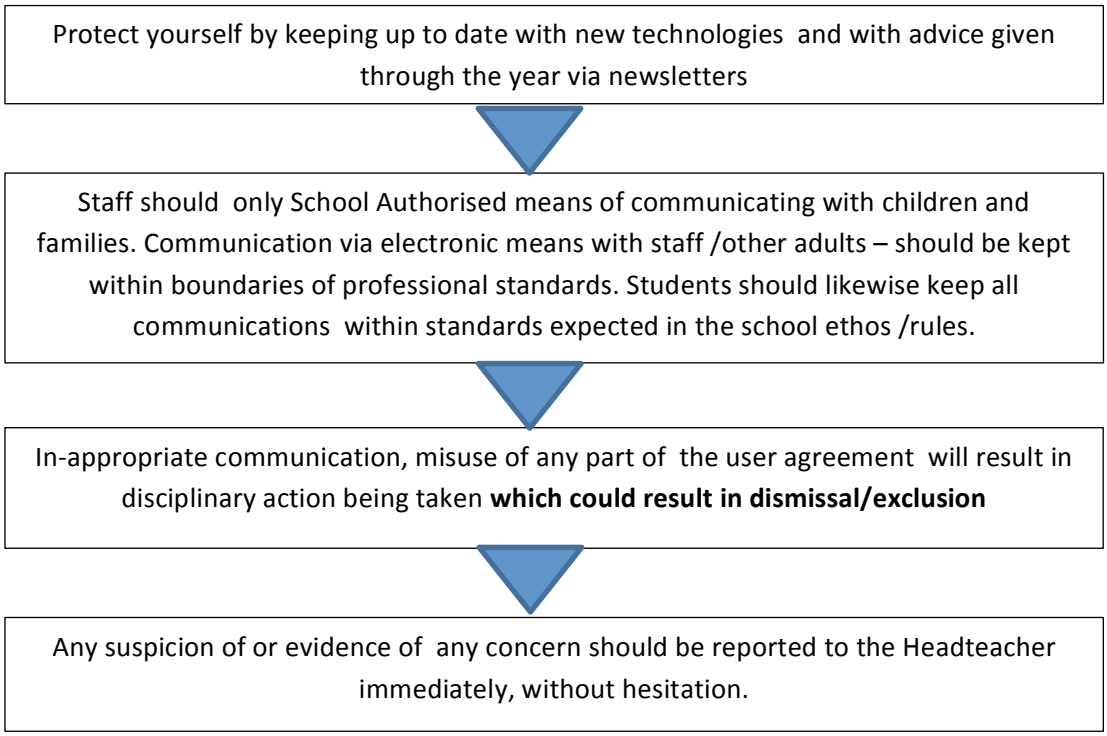
C 15 - E SAFETY & ICT USE POLICY



E-Safety encompasses internet technologies and electronic communications such as mobile telephones and wireless technology. Use of the school's ICT equipment by any members of the school community must be in accordance with this policy. Any use which infringes this policy will be treated very seriously by the School Governing Body. The school's E-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

Teaching and Learning - The Importance of Internet use in Education

• The internet is an essential element in 21st Century

• Internet use is part of the statutory curriculum and a necessary tool for staff and students life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

• The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information systems.

Using the Internet to Enhance Learning

• Internet access in school will be designed expressly for student use and will include filtering arrangements appropriate to the age of students.

• Students will be taught in their lessons what Internet use is acceptable and what is not and given clear objectives for Internet use.

• Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

The need for students to learn to evaluate online content

• The school should ensure that the use of Internet derived materials by staff and by students complies with copyright law.

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

• If staff or students discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the School Network Manager.

The Management of Internet Access

• The school ICT system capacity and security will be reviewed regularly.

• Virus protection will be installed and updated regularly.

• Security packages will be installed

E-Mail

• Students may only use approved e-mail accounts on the school system.

• Students must immediately tell a teacher if they receive an offensive e-mail.

• Students must not reveal details of themselves or others such as address or telephone number, or arrange to meet anyone in any e-mail communication without specific permission.

• Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

• E-mail sent to an external organisation should be written carefully and authorised before sending in the same way as a letter written on school headed notepaper.

• Students should use the school email system for work and educational purposes and NOT for personal chat or for social networking.

• Staff should only use their school email account (…@stgeorgesblackpool.sch.uk) when communicating with students and parents.

• The forwarding of chain letters is not permitted.

Published content and the school website

• The contact details on the website should be the school address, school e-mail and telephone number. Staff and student home information will not be published.

• The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing student images and work

• Website photographs that include students will be selected carefully

• Students full names will not be used anywhere on the school website, particularly in association with photographs

• Written permission from parents or carers will be obtained before photographs of students are published on the school website (via admission form)

Social networking and personal publishing

• School will block access to social networking sites.

• Newsgroups will not be made available to students unless an educational requirement for their use has been demonstrated

• Students will be advised never to give out personal details of any kind which may identify them or their location

• Staff and students must not place personal photos on any social network space without considering how the photo could be used now or in the future

• Staff and Students should be advised on security and encouraged to set ‘smart’ passwords, deny access to unknown individuals and how to block unwanted communications

• It is the responsibility of the staff and student not to pass on their username and password for others to use their account

• Staff should be aware of the potential risk to their professional reputation by adding students, parents or friends of students as ‘friends’ on their social network site and are strongly recommended not to do so

• Comments made on a social network site or Blog which relate to the school or students in the school have the potential to be misinterpreted and would result in disciplinary action.

Action you must take if you discover inappropriate (threatening or malicious) material online concerning yourself or your school:

• **Secure and preserve any evidence.** For example, note the web address (URL) or stay with the computer- until further advice sort. DO NOT COPY or screen shot.

• Staff should report immediately to a line manager or senior staff

• Students should report immediately to their parents/guardians if an issue occurs at home

• Parents should contact the uploader of the material or the Internet Service Provider/ site administrator and ask for the material to be removed. All social network sites have the means to report unacceptable material or activity on their site – some more readily available than others

• Inform Headetacher/DSL

Managing Filtering

• The school will work in partnership with the CIDARI MAT, DfE and the Internet Service Provider to ensure systems to protect students are reviewed and improved

• If staff or students discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the School Network Manager

Support Team.

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

Managing video conferencing

• The use of video conferencing facilities in school will be for approved activities only and all such use by groups of students will be monitored carefully.

Managing emerging technologies

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

• Mobile telephones will not be used during lessons or formal school time without permission. The sending of abusive or inappropriate text messages is forbidden.

• Mobile telephones remain the responsibility of the student – if they are lost or stolen the school cannot accept liability.

• Staff will be issued with a school telephone for trips and visits out of school.

Protecting Personal Data

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

Policy Decisions/ Authorising Internet Access

• All staff and student must read and sign the Responsible Internet Use statement before using any school ICT resource.

• The school will maintain a current record of all staff and students who are granted access to school ICT systems.

• Students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement.

• Parents/carers will be asked to sign and return a consent form.

Staff who wish to BYOD:

Data must be protected and software protected. Secure passwords should be used and updated regularly – at least each term.

Any data sent out of the school system must be password protected/encrypted

The use of pen drives and other external devices is strongly discouraged , all data should be encrypted. Use of the school servers is the only save storage. Updated 'cloud' storage advice will follow - security should not be taken as granted.

Assessing Risks

• The school will take reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the Diocese can accept liability for the material accessed, or any consequences of Internet access.

• The school will audit ICT use on a regular basis to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate.

Handling E-safety Complaints (See also Statutory Policy 14)

• Complaints of Internet misuse will be dealt with by a senior member of staff.

• Any complaint about staff misuse must be referred to the Headteacher.

• Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

• Students and parents will be informed of the complaints procedure. Any illegal issues will be discussed with the police.

Community Use of the Internet

• The school will liaise with local organisations to establish a common approach to E safety.

Communications Policy

Introducing e-safety to students

• E-safety rules will be posted in all networked rooms.

• Students will be informed that network and internet use will be monitored.

Staff and the E-safety policy

• All staff will be informed of and have access to the school E-safety policy and its importance explained

• Staff should be aware the Internet traffic can be monitored and trace to the individual user. Discretion and professional conduct is essential

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

• Staff should understand that telephone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship

Enlisting parents' support

• Parents attention will be drawn to the school E-safety policy in newsletters, the school brochure and on the school website.

Non-compliance

• The school retains the right to withdraw any of the above services of the person(s) if they have been found

Appendices

1. Responsible Internet Use: Rules for Staff and Students

2. Letter to parents on Responsible Internet Use

3. Consent Form

4. Flowchart for an E-safety Concern

5. Staff Declaration

Appendix 1

Responsible Internet Use: Rules for Staff and Students

The computer system is owned by the school. This Responsible Internet Use statement helps to protect students, staff and the school by clearly stating what use of computer resources is acceptable and what is not.

Irresponsible use may result in the loss of Internet access, in line with the School's Behaviour Policy.

Network access must be made via the user's authorised account and password, which must not be given to any other person.

School computer and Internet use must be appropriate to the student's education or to staff professional activity.

Copyright and intellectual property rights must be respected. E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.

Users are responsible for e-mail they send and for contacts made.

The use of social networking sites (Facebook, etc) are not permitted on site.

Anonymous messages and chain letters are not permitted.

The use of unauthorised chat rooms is not allowed.

The school ICT systems may not be used for private purposes, unless the Headteacher has given permission for that use.

Use for personal financial gain, gambling, political purposes or advertising is not permitted. ICT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.

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

Legislation (2006) gives advice regarding 'Taxable' use of school equipment at home (eg: Laptops, IPads). Staff will need to declare the personal use of school equipment at home is minimal and insignificant, personal use in school is also rare.

Appendix 2

Dear Parents/Carers

Responsible Internet Use

As part of your child's curriculum and the development of ICT skills, St George's School is providing access to the Internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and an essential skill for all students as they grow up in the modern world. Please could you read the attached - Rules for Responsible Internet Use and sign and return the consent form so that your child may use the Internet at school. If you wish to see a full copy of the school's 'E-Safety and Acceptable Use Policy' this is available on the school website.

Although there are concerns about students potentially having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The school will not be liable for any damages arising from your child's use of the Internet facilities.

Yours sincerely

CONSENT FORM **ICT USE & ACCESS** Appendix 3

ST GEORGE'S SCHOOL **Responsible Internet Use**

Please complete, sign and return to your child's College Tutor

Student: College Gp:

I have read and I understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.

Student's Agreement

Signed: (Student) Date:

I have read and understood the school rules for responsible Internet use and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure students cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Parent's Consent for Internet Access

Signed: Date:

Please print name:

I agree that, if selected, my son/daughter's work may be published on the school website.
Parent's Consent for Web Publication of Work and Photographs

YES / NO (please circle)

I agree that photographs that include my son/daughter may be published subject to the discretion of staff and school rules.

YES / NO (please circle)

If NO: Please explain to your child, the STUDENT must be responsible to tell the teacher/member of staff if a situation occurs where their photograph is likely to be taken they must state this at the time.

Signed: Parent /Carer Date:

Appendix 4:

Flowchart for an E-safety Concern

- Establish who is involved and whether victim or perpetrator. Secure and preserve any evidence. Do not copy, print or send evidence.
- Do not switch off the computer.
- Is it in-appropriate? / illegal?
- Illegal Inappropriate / Illegal, but not safeguarding/child protection

SAFEGUARDING/CHILD PROTECTION ISSUE – child as victim and/or perpetrator?

Safeguarding and Child Protection Referral

- Risk assessment
- Counselling
- Discipline
- Referral to other agencies.
- All incidents recorded
- Use information to inform and review policies

Secure and preserve any evidence.

Initiate internal action:

- Risk assessment
- Counselling
- Discipline
- Referral to other agencies.

Appendix 5

St George's School Staff ICT /E Safety

STAFF DECLARATION:

If you have use of school computer equipment at home or work signing this declaration implies full understanding of the School ICT /ESafety Policy as described in the Core Policy Staff Handbook and any Income Tax implications.

I (Caps)……..declare that:

- Any computer equipment loaned to me from school to use at home or school is to be used solely by me for the purposes of my profession, any personal use is minimal and insignificant. No personal gain will be sought

- Personal use in school is also extremely rare.

- Any programs/software/technology/telephones/email use sourced from St George's School remains the property of the school and will be used within set boundaries.

- Access codes and personal passwords will remain confidential to the owner. If you bring (use) your own device (BYOD) – there are specific rules regarding security of school data and software. I am fully aware of these rules.

- I understand records kept will be for auditors inspection if required. Checks of accounts would take place by school management both randomly and/or if there are any suspicions that a person's actions may be a threat to the integrity of the school, staff disciplinary concerns or to E Safety. These could happen at anytime, authorised by the Headteacher, who is advised by CIDARI, LEA, Police

- I have read and understood the school policy (C15 E SAFETY & ICT USE POLICY), Breach of this Policy could have serious disciplinary consequences up to and including dismissal.

I fully understand and agree to abide by the set procedures and will ask if unsure.

Signed: …… ……Date: ……

This declaration will be held for inspection by Income Tax Authorities.