Sir Robert Geffery's School

E-Safety Policy
And
Acceptable Use Agreement

SIR ROBERT GEFFERY'S SCHOOL
E-SAFETY POLICY

Ethos

At Sir Robert Geffery's School we ensure that through our school vision, values, rules, diverse curriculum and teaching we promote tolerance and respect for all cultures, faiths and lifestyles. The governing body also ensures that this ethos is reflected and implemented effectively in school policy and practice and that there are effective risk assessments in place to safeguard and promote students' welfare.

We have a duty to prepare our children for life in modern Britain and to keep them safe.

Pupils who attend our school have the right to learn in safety. We do not tolerate bullying of any kind and will challenge derogatory language and behaviour towards others.

Introduction

Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the every day lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our children with the skills to access life-long learning and employment.

Computing covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of Computing within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming

- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality such as Smartwatches

Whilst exciting and beneficial both in and out of the context of education, much Computing, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Sir Robert Geffery's School we understand the responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy is inclusive of both fixed and mobile internet; technologies provided by the school; (such as PCs, laptops, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff (such as laptops, mobile phones, camera phones and portable media players, etc). Valuable items should not be brought into school, as the school is not responsible for any loss of items.

The school is aware of the constant development in technology and keeping up-to-date with developments, which must be addressed in e-Safety education.

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinator in our school is Mrs Curtis. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety coordinator to keep abreast of current issues and guidance through organisations such Cornwall LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

The Head/e-Safety coordinator updates Senior Management and Governors and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Writing and reviewing the e-Safety Policy

This policy, supported by the school's Acceptable Use Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies including those for Computing, Home-school agreements, Behaviour, Health and Safety, Child Protection, and PSHE policies including Anti-bullying.

Our e-Safety Policy has been written by the school, in conjunction with advice from Cornwall Council, Swgfl, Becta and government guidance. It has been agreed by the Senior

Management Team, Staff and approved by the Governing Body. The e-Safety policy and its implementation will be reviewed annually.

E-Safety skills development for staff

- Our staff receive regular information and training on e-Safety issues through the coordinator at staff meetings.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff receive information on the school's Acceptable Use Agreement as part of their induction.
- All staff are encouraged to incorporate e-Safety activities and awareness within their lessons.

E-Safety information for parents/carers

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website
- The school holds regular e-Safety workshops for parents
- The school sends out relevant e-Safety information to parents through newsletters and posts information on the School Website.

Community use of the Internet

- External organisations using the school's Computing facilities must adhere to the e-Safety policy.

4. Teaching and Learning

Internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas to teach e-Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.

- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

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

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

3. Managing Internet Access

Information system security

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- School Computing systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Cornwall Council.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- 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 paper.
- The forwarding of chain letters is not permitted.

Published content and the school web site

The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will **not** be published. The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully
- Pupils' full names will not be used anywhere on the Sir Robert Geffery's School Website, particularly in association with photographs.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

Photographs taken by parents/carers for personal use

In the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites and social media, e.g. School performances and assemblies etc. Parents/ carers will be asked to sign a form agreeing to this when attending such events.

Social networking and personal publishing

- The school will block / filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. Children will still be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of cyber bullying to the school.
- School staff are advised about security settings and advised not to add children as 'friends' if they use these sites.

Managing filtering

- The school will work with the LA, DFE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If pupils or staff discover an unsuitable site, it must be reported to the Class Teacher or Headteacher.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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.
- The use of portable media such as memory sticks and CD ROMS will be monitored closely as potential sources of computer virus and inappropriate material.
- Pupils are not allowed to bring personal mobile devices/phones to school. Any phones that are brought to school will be sent to the school office and kept there until the end of the day.
- The sending of abusive or inappropriate text messages outside school is forbidden.
- Staff will use a school phone where contact with pupils is required.
- Staff should not use personal mobile phones during designated teaching sessions. When their use is necessary this should only take place within the office or staff room – not around pupils in the school building.

Managing video-conferencing

- When it is used in our school, videoconferencing and skype uses the educational broadband network to ensure quality of service and security rather than the Internet.
- Video-conferencing will be appropriately supervised for all pupils' age.

Protecting personal data

The school will collect personal information about you fairly and will let you know how the school, DFE and Cornwall LA will use it. The school will use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond the school, DFE or Cornwall LA. For other members of the community the school will tell you in advance if it is necessary to pass the information on to anyone else other than the school, DFE and Cornwall LA.

The school will hold personal information on its systems for as long as you remain a member of the school community and remove it in the event of you leaving or until it is no longer required for the legitimate function of the school. We will ensure that all personal information supplied is held securely, in accordance with the policies and practices of Cornwall Council and as defined by the Data Protection Act 1998.

You have the right to view the personal information that the school holds about you and to have any inaccuracies corrected.

4. Policy Decisions

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Acceptable Use Agreement for pupils and abide by the school's e-Safety rules. These e-Safety rules will also be displayed clearly in all networked rooms.
- Access to the Internet will be by directly supervised access to specific, approved on-line materials.
- All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's e-Safety rules and within the constraints detailed in the school's e-Safety policy.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school Computing resource.

Password Security

- Adult users are provided with an individual network, email password
- All pupils are provided with a class username and password.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school or Cornwall LA can accept liability for the material accessed, or any consequences of Internet access. The school will audit Computing provision to establish if the e-Safety policy is adequate and that its implementation is effective.

Handling e-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff and reported to the e-Safety coordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety coordinator and recorded in the e-Safety incident logbook.
- 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.
- Pupils and parents will be informed of the complaints procedure.

5. Communications Policy

Introducing the e-Safety policy to pupils

- E-Safety rules will be displayed in all classrooms and discussed with the pupils at. Specific lessons will be taught by class teachers at relevant points throughout e.g. during PSHE lessons/circle times/anti-bullying week.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the e-Safety policy

- All staff will be given the School e-Safety policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

6. **Monitoring and review**

This policy is implemented on a day-to-day basis by all school staff and is monitored by the e-Safety Coordinator.

This policy is the Governors' responsibility and they will review its effectiveness annually. They will do this during reviews conducted between the e-Safety Coordinator, Computing Coordinator, Designated Child Protection Coordinator, and Governor with responsibility for Computing and Governor with responsibility for Child Protection (e-Safety committee). Ongoing incidents will be reported to the full governing body.

The e-Safety policy will be revised by the e-Safety Coordinator.

Reviewed and Approved by Governors (Curriculum Committee) in Spring 2017

PUPIL GUIDELINES FOR SAFE INTERNET/EMAIL USE

- I will only use the Internet when there is a teacher present.
- I will always ask for permission before accessing the Internet/Email.
- I will only use my own usernames and passwords to log on to the system//email and keep them secret.
- I will not access other people's files.
- I will only email people I know, or my teacher has approved and ensure that the messages that I send will be polite and responsible.
- I understand that the use of strong language, swearing or aggressive behaviour is not allowed when using Email etc.
- I will not give personal details (like my home address, telephone or mobile number), or the personal details of any other person to anyone, or arrange to meet someone unless my parent/carer or teacher has given me permission.
- I will only download, use or upload material when I have been given the owner's permission.
- I will only view, download, store or upload material that is lawful, and appropriate for other users. If I am not sure about this, or come across any potentially offensive materials, I will use the 'Hector Protector' button and inform my class teacher straight away.
- I will avoid any acts of vandalism. This includes, but is not limited to, uploading or creating computer viruses and mischievously deleting or altering data from its place of storage.
- Always quote the source of any information gained from the Internet i.e. the web address, in the documents you produce.
- Use the Internet for research and school purposes only.
- I will not bring in memory sticks or CD Roms from home to use in school unless I have been given permission by my class teacher.
- I understand that the school may check my computer files/Emails and may monitor the Internet sites that I visit.
- I understand that if I don't follow these rules, my access to the school computer system/Internet/Email may be suspended, and my parents/carers will be informed.

SIR ROBERT GEFFERY'S SCHOOL

Acceptable Use Agreement
For Pupils

Please complete and return this form to your child's class teacher

Pupil's Name		**Class Teacher**	
As a school user of the Internet, I agree to follow the school rules on its' use. I will use the network in a responsible way and observe all the restrictions explained to me by my school.			
Pupil Name (print)			
Pupil Signature		**Date**	

Parents Name			
As the parent or legal guardian of the pupil above, I give permission for my son or daughter to use the Internet, including Email. I understand that pupils will be held accountable for their own actions. I also understand that some of the materials on the Internet may be unsuitable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information.			
Parents Name (print)			
Parents Signature		**Date**	

SIR ROBERT GEFFERY'S SCHOOL

Acceptable Use Agreement
For Staff

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties – the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff requesting Internet access should sign a copy of this Acceptable Internet Use Statement and return it to the Head Teacher for approval.

- All Internet activity should be appropriate to staff professional activity or the student's education
- Access should only be made via the authorised account and password, which should not be made available to any other person
- Activity that threatens the integrity of the school Computing systems, or activity that attacks or corrupts other systems, is forbidden
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Copyright of materials must be respected
- Posting anonymous messages and forwarding chain letters is forbidden
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden

Name		
Date		**Signed**

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	√						√	
Use of mobile phones in lessons				√				√
Use of mobile phones in social time	√						√	
Taking photos on mobile phones or other camera devices	√						√	
Use of hand held devices eg PDAs, PSPs		√					√	
Use of personal email addresses in school, or on school network	√							√
Use of school email for personal emails	√							√
Use of chat rooms / facilities				√				√
Use of instant messaging				√				√
Use of social networking sites				√				√
Use of blogs		√				√		

When using communication technologies the school considers the following as good practice:

- **The official school email service may be regarded as safe and secure and is monitored.** *Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).*
- **Users need to be aware that email communications may be monitored**
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.**
- **Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.*
- *Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.*
- *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restrComputings certain internet usage as follows:

User Actions		Acceptable	Acceptable at	Acceptable	Unacceptable	Unacceptable
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**child sexual abuse images**					☐
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					☐
	adult material that potentially breaches the Obscene Publications Act in the UK					☐
	criminally racist material in UK					☐
	pornography				☐	
	promotion of any kind of discrimination				☐	
	promotion of racial or religious hatred				☐	
	threatening behaviour, including promotion of physical violence or mental harm				☐	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				☐	
Using school systems to run a private business					☐	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					☐	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					☐	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					☐	
Creating or propagating computer viruses or other harmful files					☐	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					☐	
On-line gaming (educational)		√				
On-line gaming (non educational)					√	
On-line gambling					√	
On-line shopping / commerce					√	
File sharing					√	
Use of social networking sites					√	
Use of video broadcasting eg Youtube					√	

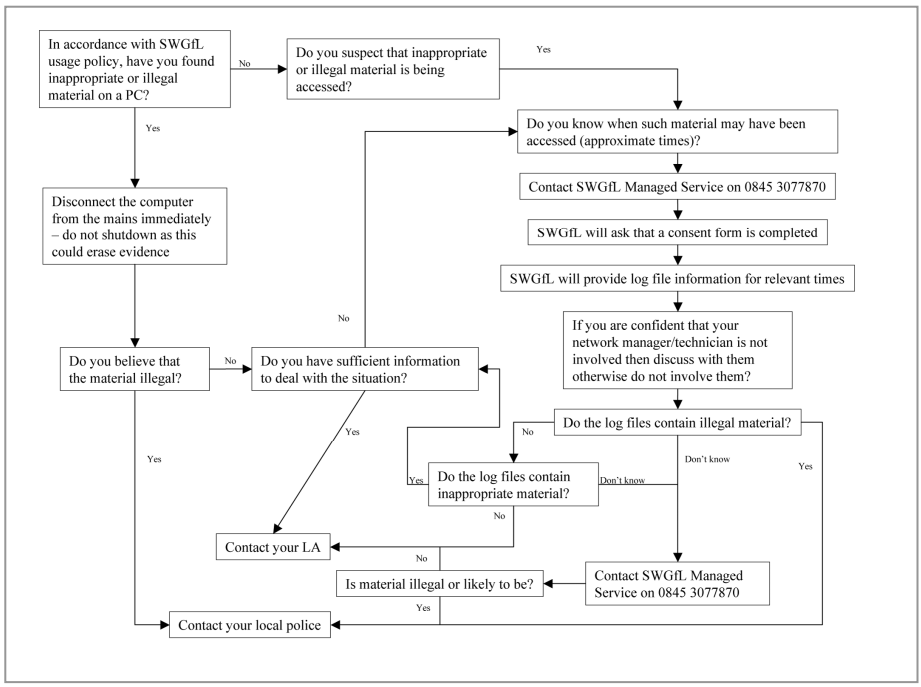
Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of Computing, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- **child sexual abuse images**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

the SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students / Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		□	□	□		√			
Unauthorised use of non-educational sites during lessons	√								
Unauthorised use of mobile phone / digital camera / other handheld device	√								
Unauthorised use of social networking / instant messaging / personal email			√						
Unauthorised downloading or uploading of files	√								
Allowing others to access school network by sharing username and passwords	√								
Attempting to access or accessing the school network, using another student's / pupil's account	√								
Attempting to access or accessing the school network, using the account of a member of staff	√								
Corrupting or destroying the data of other users	√								
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature			√	√					
Continued infringements of the above, following previous warnings or sanctions				√					
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			√						
Using proxy sites or other means to subvert the school's filtering system			√						
Accidentally accessing offensive or pornographic material and failing to report the incident			√		√				
Deliberately accessing or trying to access offensive or pornographic material			√	√					
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	√								

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		□	□	□				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		√						
Unauthorised downloading or uploading of files		√						
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		√						
Careless use of personal data eg holding or transferring data in an insecure manner		√						
Deliberate actions to breach data protection or network security rules		√						
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		√						
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		√						
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		√						
Actions which could compromise the staff member's professional standing		√						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		√						
Using proxy sites or other means to subvert the school's filtering system		√						
Accidentally accessing offensive or pornographic material and failing to report the incident		√						
Deliberately accessing or trying to access offensive or pornographic material				√				
Breaching copyright or licensing regulations		√						
Continued infringements of the above, following previous warnings or sanctions				√				