Westbury C.E. Junior School
Draft E-Safety Policy
(For Consultation)

January 2015

Contents

Draft E-Safety Policy for Discussion

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care we provide as a school. We believe that the development and implementation of such a strategy should involve all the stakeholders in a child's education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

There is no doubt that the use of these exciting and innovative tools both in school and at home can help raise educational standards and promote pupil achievement.

However, the use of these new technologies can also put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games and other content
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect similar situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies) to ensure the proper safeguarding of pupils.

As with all other risks, it is impossible to eliminate risk completely. It is therefore essential, through good educational provision to also build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

We believe that the school must demonstrate that it has provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development, Monitoring and Policy Review

This e-safety policy has been developed by consultation with:

- *Headteacher / Senior Leaders*
- *Teachers*
- *Support Staff*
- *ICT Technical staff*
- *Governors*
- *Parents and Carers*
- *Community users*

As well as this Cconsultation has taken place with the whole school community through the following:

- *Staff meetings*
- *Schooll Council*
- *INSET Day*
- *Governors meeting*

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *Governors on:*	*Insert date*
The implementation of this e-safety policy will be monitored by the:	
Monitoring will take place at regular intervals:	*One a year recommended*
The Governors will receive a report on the implementation of the e-safety policy (which will include anonymous details of e-safety incidents) at regular intervals:	*One a year recommended as a minimum.*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*Date of next review*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*Relevant agancies: LA. Police etc*

The school will also monitor the impact of the policy using:

- *Surveys / questionnaires of*
  - *students / pupils (eg Ofsted "Tell-us" survey / CEOP ThinkUknow survey)*
  - parents / carers
  - staff

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place outside of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out through the receiving of regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of *E-Safety Governor* . The role of the E-Safety Governor will include:

- Computing subject leader provides a report for the relevant Governor / meeting

Headteacher and Senior Leaders:

- **The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community**, though the day to day responsibility for e-safety will be delegated to the technical support and computing subject leader
- The leadership team are responsible for ensuring that the relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The leadership team will receive regular monitoring reports from the computing subject leader

  The Headteacher will be aware of who is teaching computers within the school if not the class teacher.
- **The Headteacher and Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.** See Child protection policy

Computing Subject Leader

–In this role they:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and associated documents

- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school IT staff
- Contacts regularly with the Governor with computing responsibility to discuss current issues
- reports regularly to Leadership Team

Technical Support

Via the computing subject leader, is responsible for ensuring:

- that the school's IT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- SWGfL is informed of issues relating to the filtering applied by the Grid
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network and email is regularly monitored in order that any misuse / attempted misuse can be reported to the **headteacher** for investigation and sanction where appropriate.
- that monitoring systems are implemented and updated as agreed in school policies

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the headteacher for investigation and sanction where appropriate
- digital communications with pupils/ parents/ carers (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities and e-safety rules will be displayed throughout school.
- pupils understand and follow the school e-safety and acceptable use guidelines
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated person for child protection

should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

  To sign the home school agreement
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and other digital devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website, info from national / local e-safety campaigns*

Parents and carers will be responsible for:

- To sign the home school agreement
- accessing the school website, on-line pupil records and other school related digital documents in accordance with the relevant school policies

Policy Statements

Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT and PHSE and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and classroom activities
- pupils should be taught in all lessons, where on-line content is used, to be critically aware of the content they access and be guided to validate the accuracy of information
- Staff should act as good role models **i**n their use of ICT, the internet and mobile devices

Education – parents / carers

We acknowledge that some parents and carers may have only a limited understanding of e-safety risks and issues, yet play an essential role in the education of their children and in the monitoring of their on-line experiences. This can mean that they either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and can often be unsure about what they should do about it.

Therefore, the school will seek to provide information and awareness to parents and carers through:

- Letters, newsletters and our website
- Parents meetings

- Reference to the SWGfL Safe website rules

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy
- *This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.*
- *The computing subject leader will provide advice / guidance / training as required to individuals as required*

Training – Governors

Governors should take part in e-safety training and awareness sessions, with particular importance for those who are involved in ICT and e-safety within the school. This may be offered in a number of ways:

- Participation of Local or National e safety courses and training
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and any relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted as much as is possible
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the office manager and will be reviewed annually at least by the Leadership Team
- The “administrator” passwords for the school ICT systems, used by the Office Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place
- Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details
- The school maintains and supports the managed filtering service provided by SWGfL
- Any need to switch off the filtering, will be carried out by a process that is agreed by the Headteacher
- Any filtering issues should be reported immediately to SWGfL.
- *Appropriate security measures are in place* E.G. passwords, locks, security markings etc) *to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.*
- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, visitors) onto the school system*.*
- An agreed policy is in place regarding the extent of personal use that users and their family members are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy is in place (would need to briefly outline how) that allows staff to install programmes on school workstations / portable devices.

- An agreed policy is in place (Briefly outline) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations and portable devices.
- *The school infrastructure and individual workstations are protected by up to date virus software. (Sofos)*
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- *in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*
- *Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.*
- *It is accepted that from time to time, for good educational reasons, staff and students may need to access sites that may be blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study.. Any request to do so, will be recorded, with clear reasons for the need. You tube is available in school through the proxy server and staff are aware of their responsibility to watch clips before sharing with pupils and that pupils will not be allowed to use the site.*
- *Pupils should be taught in all lessons* to be critically aware of the content they access on-line and be guided to validate the accuracy of information

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils the instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm. This includes:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use and sharing of images
- *Staff are allowed to take* digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes. These images should also only be stored on school equipment and deleted as soon as used for their original purpose. No images of children should be stored unless required for educational, school related purposes at a later date. Images of children may be stored in the relevant folder on staff share for the duration of that cohort of children's time at the school. Year group folders will be deleted once the year group leaves.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Staff and pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- *Pupils' full names will not be used anywhere on our website, particularly in association with photographs.*
- *Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website*
- *Pupil's work can only be* published with the permission of the pupil and parents or carers

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes

- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject’s rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed
Use of mobile phones in lessons		X		
Use of mobile phones in social time	X			
Taking photos on mobile phones Taking photos on school camera	 X			X
Use of personal email addresses in school, or on school network		X		
Use of school email for personal emails		X		
Use of chat rooms / facilities		X		
Use of instant messaging		X		
Use of social networking sites		X		
Use of blogs		X		

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 restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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					X
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					X
	adult material that potentially breaches the Obscene Publications Act in the UK					X
	criminally racist material in UK					X
	pornography				X	
	promotion of any kind of discrimination				X	
	promotion of racial or religious hatred				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	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				X	
Using school systems to run a private business					X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
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					X	
On-line gaming (educational)				X		

On-line gaming (non educational)				X	
On-line gambling				X	
On-line shopping / commerce		X			
File sharing		X			
Use of social networking sites		X			
Use of video broadcasting eg Youtube				X	

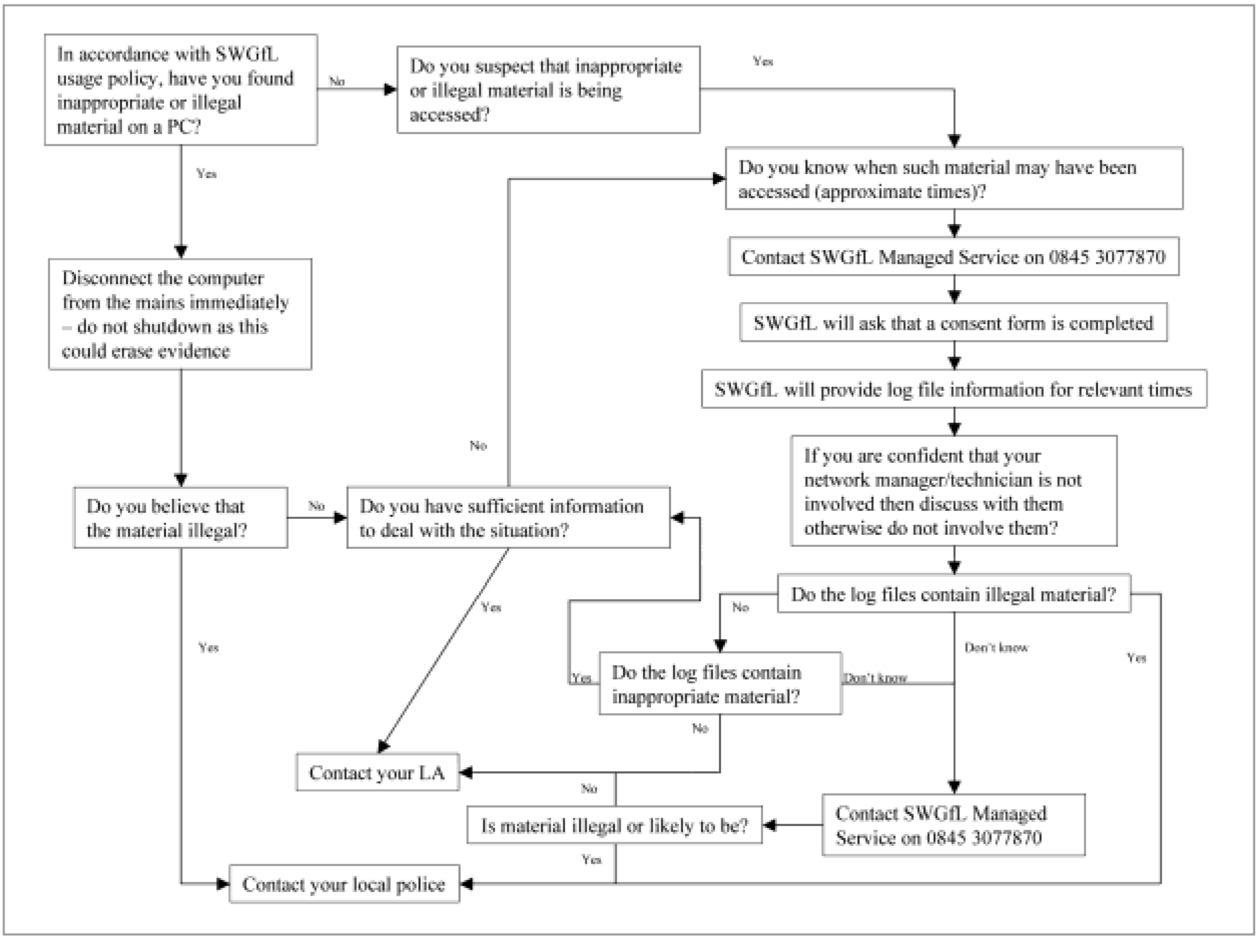
Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, 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

Then we can follow the procedures outlined in the SWGfL flow chart . In our authority this is recommended to be consulted and followed, in particular those sections on reporting the incident to the police and the preservation of evidence


In accordance with SWGfL usage policy, have you found inappropriate or illegal material on a PC?
No
Do you suspect that inappropriate or illegal material is being accessed?
Yes
Yes
Do you know when such material may have been accessed (approximate times)?
Contact SWGfL Managed Service on 0845 3077870
SWGfL will ask that a consent form is completed
SWGfL will provide log file information for relevant times
Disconnect the computer from the mains immediately – do not shutdown as this could erase evidence
No
If you are confident that your network manager/technician is not involved then discuss with them otherwise do not involve them?
Do you believe that the material illegal?
No
Do you have sufficient information to deal with the situation?
Do the log files contain illegal material?
Yes
No
Yes
Don't know
Yes
Yes
Do the log files contain inappropriate material?
Don't know
No
Contact your LA
No
Is material illegal or likely to be?
Contact SWGfL Managed Service on 0845 3077870
Yes
Contact your local police

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal, it is essential that correct procedures are used to investigate.

It is envisaged that the school is more likely to deal with incidents that involve inappropriate rather than illegal misuse. We firmly believe it is crucial 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 /

Staff Actions / Sanctions

Incidents:	Refer to computer subject leader	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		√	√	√	√		√	√