Brownsover Community School

Online Safety Policy

Policy Number	C11a - Curriculum
Prepared By	Sarah Halliwell
Acknowledgement(s)	Staff
Last Date Approved	January 2023
Effective Date	January 2023
Physical Location of Policy	Curriculum file in HT office
Date of Next Review	January 2024
	Online Safety to be reviewed annually. Next review: Jan 2024

Document Information

Document history

Version no.	Date	Change
1.6	Jan 2019	Updated to include GDPR requirements
1.7	Jan 2020	No changes made
1.8	Jan 22	Governor organisation amended
1.9	Jan 23	Named staff/Govs updated, Safeguarding aspect updated.

Approvals

Role	Name	Signature / Approval	Date
Headteacher	E. Basnett		Jan 23
Governors - Full Governing Body	L Flavell/R Street		Feb 23
Governor			

Reviewers

Role	Name
Head teacher	E. Basnett
SLT	
Governors	
staff	Teaching staff, Sophie Mahloudji, GDPR Champion Elaine Murray

Distribution for Information

Role	Name

Brownsover Community School

Acceptable Internet Use Statement

For Staff

The computer system is owned by the school and is made available to students to further their education and 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 read and agree this Acceptable Internet Use Statement. This is done as part of new staff induction.

- All Internet activity should be appropriate to staff professional activity;
- 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 ICT 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.
- The use of Facebook or other social networking sites is forbidden on school premises. Staff should not refer to any child or staff member when using these sites outside of school and should maintain professional conduct at all times. The only exception to this is approved staff responsible for our school Facebook account.

Brownsover Community School Online Safety Policy

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. Electronic communication helps teachers and *children* learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children should have an entitlement to safe internet access at all times.

The requirement to ensure that children are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school online safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve everyone in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the children themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote children's achievement.

However, the use of these new technologies can put children 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
- 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 situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / 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.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The online 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 / Review of this Policy

This online safety policy has been developed by a working group / committee made up of:

- *School Online Safety Coordinator*
- *Headteacher / Senior Leaders*
- *Teachers*
- *Support Staff*
- *ICT Technical staff (Launch ICT)*
- *Governors*
- *Parents and Carers*
- *Community users (Bridges)*

Consultation with the whole school community has taken place through the following:

- *Staff meetings*
- *School Council*
- *INSET*
- *Governors meeting*
- *Parents evening*
- *School website / newsletters*

Schedule for Development / Monitoring / Review

This online safety policy was approved by the *Governing Body / Governors Sub Committee on:*	*July 2015*
The implementation of this online safety policy will be monitored by the:	*Online Safety Coordinator, Senior Leadership Team and Head Teacher*
Monitoring will take place at regular intervals:	*January each year*
The *Governing Body / Governors Sub Committee* will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*January each year*
The Online 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 online safety or incidents that have taken place. The next anticipated review date will be:	*January each year*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*LA ICT Manager, LA Safeguarding Officer, Police Commissioner's Office*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Internal monitoring data for network activity*
- *Surveys / questionnaires of*
  - *Children / school council (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, children, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

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

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving information about online safety incidents and monitoring reports. A member of the Governing Body will take on the role of *Online Safety Governor* (Rachel Street & Lucy Flavell)

The role of the Online Safety Governor will include:

- *Annual meetings with the Online Safety Co-ordinator / Officer*
- *Continuous monitoring of online safety incident logs in conjunction with other logs to check for patterns*
- *Annual monitoring of filtering / change control logs*
- *Annual reporting to relevant Governors meeting*

Headteacher and Senior Leaders:

- **The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community**, though the day to day responsibility for online safety will be delegated to the Online *Safety Co-ordinator.*
- *The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant*
- *The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.* – (The LA)
- **The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.**

Online Safety Coordinator / Officer:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets annually with Online Safety Governor to discuss current issues and review incident logs
- attends relevant meeting / committee of Governors
- reports incidents to Senior Leadership Team

Network Manager / Technical staff:

The Network Manager (Launch ICT)

- **Will check that the school's ICT infrastructure is secure and is not open to misuse or malicious attack**
- **Making sure that the school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance**
- **Ensuring 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
- *Maintaining the school's filtering policy, that it is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person*
- Checking that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- *Monitoring software / 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 online safety policy and practices**
- **they report any suspected misuse or problem to the online safety Co-ordinator / Headteacher for investigation / action / sanction**
- online safety issues are embedded in all aspects of the curriculum and other school activities
- children understand and follow the school online safety and acceptable use policy
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of online 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, children 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 (zip it, block it, flag it)*

Designated person for safeguarding (DSL)

should be trained in online 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

(nb. it is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop. Some schools may choose to combine the role of safeguarding officer and online safety officer)

Online Safety Committee

Members of the online safety *committee* (school council) will assist the online safety *Coordinator* with:

- finding ways of promoting online safety within the school
- *reviewing the effectiveness of online safety*

Students / pupils:

- **are responsible for using the school ICT systems in accordance with the Children's I can statements on how to stay safe online which are displayed and shared regularly.**
- 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.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety Policy covers their actions out of school too.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile 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 / VLE and information about national / local online safety campaigns / literature*

Policy Statements

Education – Children

Whilst regulation and technical solutions are very important, their use must be balanced by educating *children* to take a responsible approach. The education of *children* in online safety is therefore an essential part of the school's online safety provision. Children need the help and support of the school to recognise and avoid online safety risks and build their resilience.
online safety education will be provided in the following ways:

- **A planned online safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school**
- **Key online safety messages should be reinforced as part of a planned programme of assemblies and online safety days.**

Education – parents / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).
The school will therefore seek to provide information and awareness to parents and carers through:

- *Letters, newsletters, web site*
- *A chance to share the children's* online safety *work*
- *Reference to the SWGfL Safe website and also the Online Safety Guidance for Parents*

Education & Training – Staff

It is essential that staff receive online safety updates and understand their responsibilities, as outlined in this policy.

- **All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies**
- *The* online safety *Coordinator will receive regular updates through attendance at SWGfL / LA / other information / training sessions and by reviewing guidance documents released by BECTA / SWGfL / LA and others.*

- *This* online safety *policy and its updates will be presented to and discussed by staff, when required.*
- *The* online safety *Coordinator will provide advice / guidance / training as required to individuals as required*

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members who are actively involved with e-safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / SWGfL or other relevant organisation.
- 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 infrastructure / 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 that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority online 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. (locked box)**
- **All users will have clearly defined access rights to school ICT systems.**
- **The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)**
- *Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security/GDPR*
- *The school maintains and supports the managed filtering service provided by WES*
- *Any filtering issues should be reported immediately to WES*
- *An appropriate system is in place* (incident log) *for users to report any actual /* potential online safety incident.
- *Appropriate security measures are in place 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.*
- *The school infrastructure and individual workstations are protected by up to date virus software.*
- *Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*

Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

- *Where students are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the children visit.*

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff and children 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:

- **When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.**
- *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. This is subject to the consent received on our updated GDPR forms from parents. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.*
- *Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*
- *Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images and on consent.*
- *Children's 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 / pupils are published on the school website*
- *Children's work can only be published with the permission of the student / pupil and parents or carers.*

Data Protection (GDPR)

Personal data will be recorded, processed, transferred and made available following the changes in law with the Data Protection Act and the General Data Protection Regulations (GDPR) which came into effect in 2018. This change has ensured higher standards for handling data and greater expectations for improved transparency, enhanced data security and increased accountability for processing personal data.

The GDPR principles require that all personal data shall be:

(1) processed lawfully, fairly and in a transparent manner

(2) used for specified, explicit and legitimate purposes

(3) used in a way that is adequate, relevant and limited to what is necessary

(4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, is erased or rectified without delay

(5) kept no longer than is necessary

(6) processed in a manner that ensures it is safe and secure, ensuring that measures against unauthorised or unlawful processing and against accidental loss, destruction or damage are in place

Staff must ensure they comply with the following:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Follow our clear desks policy by keeping desks, classroom areas and photocopying areas free of confidential information.
- Follow our clear screens policy and always lock workstations when staff are away from them.
- 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.

- Follow our safe storage rules of electronic information and only save data on One Drive, encrypted USB drives and the BCS network. Ensure that transfer of data uses encryption and secure password protected devices.
- Always log off and never use the 'remember me' option to save the username and password.

For more information see our Data Protection Policy. (O5)

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

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device once it is not needed

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				Children			
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	x							x
Use of mobile phones in lessons				x				x
Use of mobile phones in social time		x						x
Taking photos on mobile phones or other camera devices				x				x
Use of hand held devices eg iPads		x						x
Use of personal email addresses in school, or on school network				x				x
Use of school email for personal emails		x						x
Use of chat rooms / facilities				x				x
Use of instant messaging				x				x
Use of social networking sites				x				x
Use of blogs				x				x

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 should therefore use only the school email service to communicate with others when in school.*
- **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.**

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			
Use of social networking sites		X			
Use of video broadcasting eg Youtube	X				

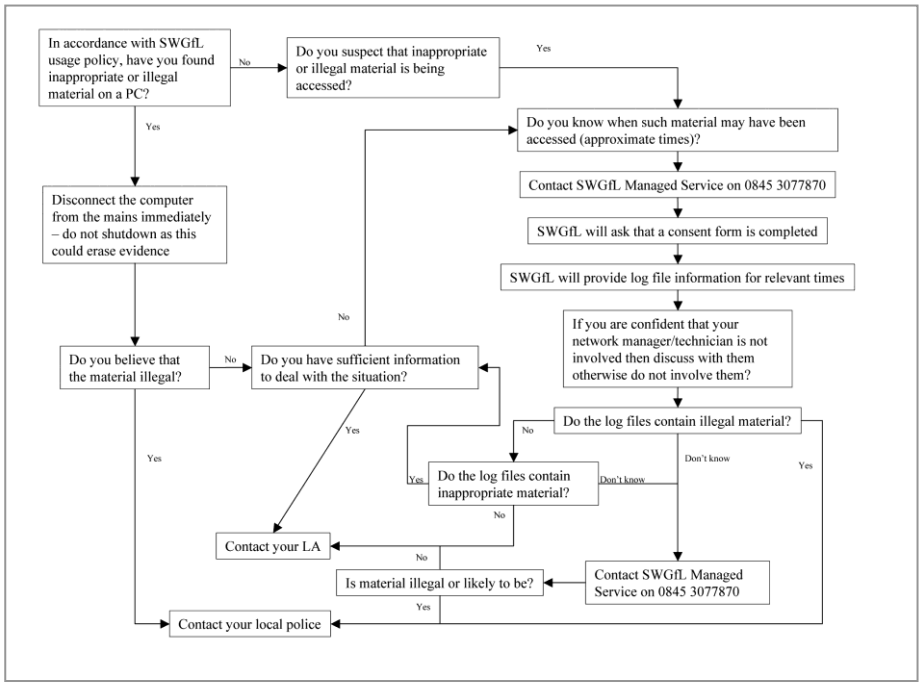
Responding to incidents of misuse

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**

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.



Sanctions

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 in line with the behaviour policy, and that members of the school community are aware that incidents have been dealt with by logging them in the eSafety incident book. 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	Refer to eSafety co-ordinator	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 (loss of play)
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		x	x	x					
Unauthorised use of non-educational sites during lessons	x					x			
Unauthorised use of mobile phone / digital camera / other handheld device		x	x			x			
Unauthorised use of social networking / instant messaging / personal email		x	x			x			
Unauthorised downloading or uploading of files	x							x	
Attempting to access or accessing the school network, using the account of a member of staff		x						x	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		x	x			x			
Continued infringements of the above, following previous warnings or sanctions		x	x				x		x
Accidentally accessing offensive or pornographic material and failing to report the incident		x	x			x			
Deliberately accessing or trying to access offensive or pornographic material		x	x			x			

Staff

Actions / Sanctions

Incidents:	Refer to eSafety co-ordinator	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).		x	x	x				
Unauthorised downloading or uploading of files	x							
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		x				X		
Careless use of personal data eg holding or transferring data in an insecure manner	x	x						
Deliberate actions to breach data protection or network security rules		x				X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x		x				
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		x		x		X		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		x		x				X
Actions which could compromise the staff member's professional standing		x				X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x				X		
Using proxy sites or other means to subvert the school's filtering system	x					X		
Accidentally accessing offensive or pornographic material and failing to report the incident		x						
Deliberately accessing or trying to access offensive or pornographic material	x	x		x				
Breaching copyright or licensing regulations	x							