

Brookburn Community School



Policy for E-safety

September 2021

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 students / pupils learn from each other. These technologies 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 to which all who work in schools are bound.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can 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
- 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 e-safety policy is used in conjunction with other school policies (e.g. 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.

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by

- Head teacher
- Senior Leaders
- Computing leader
- Academy councillors

- Teachers

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

- Staff meetings
- E-safety workshop for parents/ carers
- Academy councillors meeting / sub committee meeting

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Governing Body / Academy councillors Sub Committee on:	Nov 2021
The implementation of this e-safety policy will be monitored by the:	Head Teacher- S. Ferris, Computing Leader (B.Alderdice) and E-safety leader- (Sian Faulder) and SLT.
Monitoring will take place at regular intervals:	Yearly
The Governing Body / Academy councillors Sub Committee will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Yearly
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:	July 2022
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	S.Faulder / S. Ferris

The school will monitor the impact of the policy using:

- Logs of reported incidents
- SWGfL monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
- Students / pupils (e.g. 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, students / 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 Head teachers, to such extent as is reasonable, to regulate the behaviour of students / 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 out of school

Roles and Responsibilities

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

Academy councillors:

Academy councillors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Academy Council receiving regular information about e-safety incidents and monitoring reports. A member of the LINK Learning Trust has taken on the role of Safeguarding Trustee and there is also a safeguarding academy councillor. Both these roles include E safety. The role of the E-Safety Academy Councillor will include:

- Regular meetings with the E-Safety Lead
- Regular monitoring of e-safety incident logs
- Reporting to relevant Trustee so that reports are regularly made to Academy Council and the LINK Learning Trust Board.

Head teacher and Senior Leaders:

- **The Head teacher 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 E-Safety Co-ordinator / Officer.
- The Head teacher / Senior Leaders are responsible for ensuring that the E-Safety Leader and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Head teacher / 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 e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team / Senior Leadership Team will receive regular monitoring reports from the E-Safety Lead.
- **The Head teacher and the Deputy Heads 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.**

E-Safety Leader:

The E-Safety Leader is Sian Faulder and is responsible for the following:-

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / 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 ICT technical staff

- receives reports of e-safety incidents and, in cases where incidents are not logged on CPOMS, creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety/Safeguarding Academy Councillor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings of Academy Council
- Reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The / ICT Technician (One Education) and the Computing Co-ordinator is responsible for ensuring:

- **That the school's ICT 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
 - The school's filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix "Filtering Policy Template" for good practice document)
 - That he / she keeps 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 / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator / Officer / Head teacher / Senior Leader / Head of computing / computing Co-ordinator / Class teacher / Head of Year (as in the section above) for investigation / action / sanction
- That 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 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 E-Safety Leader / Head teacher / Senior Leader for investigation / action / sanction**
- **Digital communications with students / pupils (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
- Pupils understand and follow the school e-safety and acceptable use policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor computing 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 Safeguarding Leads

The DSLs at Brookburn are Schelene Ferris, Emily Henderson and Natalie Mason for Dolphins before and after school club. They:-

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

Safeguarding/E safety Academy Councillor

The Safeguarding E-safety Academy Councillor will assist the E-Safety Lead with:

- The production / review / monitoring of the school e-safety policy / documents.
- The production / review / monitoring of the school filtering systems.

Pupils:

- **are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems**
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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 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 / 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 e-safety campaigns / literature. Parents and carers will be responsible for:

- **endorsing (by signature) the Pupil Acceptable Use Policy**
- accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

Community Users

Community Users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign an AUP before being provided with Access to school systems.

Policy Statements

Education – 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 computing / PHSCE / other lessons 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 tutorial / pastoral activities**
- **Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information**
- Pupils should be helped to understand the need for the student / pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms and displayed on log-on screens
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

Many parents and carers have only a limited understanding of e-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 on-line 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: (select / delete as appropriate)

- Letters, newsletters, web site, social media platforms
- Parents evenings
- Reference to the SWGfL Safe website and other recommended websites via our school website.

Education - Extended Schools

The school will offer family learning courses in e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

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:

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety Lead 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 E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Lead will provide advice / guidance / training as required to individuals as required

Training – Academy councillors

Academy councillors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in computing / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Academy councillors 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 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.**
- **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 the e-safety co-ordinator and will be reviewed, at least annually, by the Safeguarding Academy Councillor and the Academy Council.

All pupil users will use a group log-on and passwords.

All staff users will use an individual log-on and password.

- **The “master / administrator” passwords for the school ICT system, used by the Technical support is also be available to the Head teacher and computing leader kept in the 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.
- The school maintains and supports the managed filtering service provided by MEWAN.
- The school has provided enhanced user-level filtering through the use of the (Freedom2cache) filtering programme.
- In the event of the technical support needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head teacher.
- Any filtering issues should be reported immediately to MEWAN.
- Requests from staff for sites to be removed from the filtered list will be **presented to the technician** and considered by the computing lead (Bob Alderdice) and e-safety lead (Sian Faulder) or a

member of SLT. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Academy Council.

- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy
- 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.
- An agreed policy is in place for the provision of temporary access of 'guests' (e.g. trainee teachers, visitors) onto the school system.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community 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 (in line with GDPR) regarding the use of removable media (e.g. laptops, iPads, memory sticks / CDs / DVDs) by users on school workstations / portable devices.
- 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

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, it is best practice that 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, e.g. 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, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical support (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils' 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. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. 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 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 e.g. 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. 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 pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- 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 a website or blog, particularly in association with photographs.
- Consent from parents or carers will be obtained before photographs of pupils are published on the school website as part of the AUP signed by parents or carers.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection - GDPR

The school will handle all data in line with the school's GDPR policy. 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 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, in line with school policy 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				Pupils				
				allowed	Allowed at certain	Allowed for selected	Not allowed	allowed	Allowed at certain	Allowed with staff	Not allowed	
Mobile phones may be brought into school									Allowed in school building. Left at office for duration of school day			
Use of mobile phones in social time (Lunch/ breaks)												
Taking photos on camera devices (excluding mobile phones)												
Use of hand held devices e.g. iPads												
Use of school email for personal emails												
Use of chat rooms												
Use of social networking sites												
Use of school blogs												

The school may also wish to add some policy statements about the use of communications technologies, in place of, or in addition to the above table:

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 (e.g. 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.
- If a requirement for the teaching of a specific element of the computing curriculum, whole class or group email addresses will be used at KS1 and 2
- 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

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and those 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:

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, e.g. 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 the 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 MEWAN 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 (e.g. 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 (non educational)	
On-line gambling	
On-line shopping / commerce	
File sharing	
Use of social networking sites (non educational)	
Use of video broadcasting e.g. YouTube (non educational)	

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.

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, preserve evidence and protect those carrying out the investigation

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:

Incident:										
	Refer to class teacher	Refer to KS leader	Refer to deputy or head	Refer to school DPO	Inform parents/carers	Refer to police	warning	Removal of network/internet access rights	Refer to tech support to adjust filters	Further sanction in line with discipline policy
Deliberately accessing or trying to access material that could be considered illegal										
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 e mail		✓			✓					
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.	✓			✓		✓			