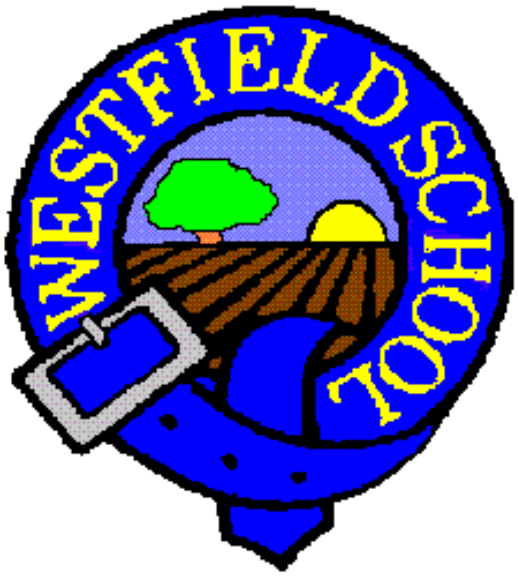
E-Safety Policy



Melanie Harbottle E safety Coordinator

Rob Gutherless ICT Governor

Policy Review: May 2017

Why we need an e-safety policy

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 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. Our school e-safety policy therefore should help to ensure safe and appropriate use. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil 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 (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 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.

Westfield Primary 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 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.

Monitoring

This e-safety policy was approved by the *Governing Body on:*	
The implementation of this e-safety policy will be monitored by the:	*M. Harbottle – E-safety Coordinator* *S. Hickey – Headteacher* *R. Gutherless – ICT Governor*
Monitoring will take place at regular intervals:	*Annually*
The *Governing Body* 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:	*Incorporated into safeguarding report*
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:	*Reviewed - May 2017*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*Primary Tech 01482 420165*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Core IS/ERYC monitoring logs of internet activity – monthly / half termly
- Internal monitoring data for network activity
- Surveys / questionnaires of pupils, parents / carers and staff

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers and visitors) 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 out of school.

Roles and Responsibility

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 by the Governors receiving 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:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meetings

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 E-Safety Co-ordinator
- The Headteacher is responsible for ensuring that the E-Safety Coordinator 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 Headteacher and SLT 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 will receive regular monitoring reports from the E-Safety Co-ordinator
- 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 e-safety allegation being made against a member of staff. E-safety training is carried out by ERYC and can booked by the CPD booking system

E-Safety Coordinator

- 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 creates a log of incidents to inform future e-safety developments,
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Senior Leadership Team
- attends relevant meeting / committee of Governors

Network Manager / Technical staff:

The ICT support supplier/ICT Co-ordinator is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the school's networks through a properly enforced password protection policy.
- ERYC IT is informed of issues relating to the filtering applied by the filtering provider
- 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 /Headteacher/ Class teacher for investigation / action / sanction

Teaching and Support Staff

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 and understood the school Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator /Headteacher / Senior Leadership Team / ICT Co-ordinator / Class teacher for investigation / action / sanction
- digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level.
- 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 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

Child Protection Officer

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:

- 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 it is expected that parents / carers would also sign on behalf of the pupils
- 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 to be considered). 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' newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

- endorsing the Pupil Acceptable Use Policy
- accessing the school website in accordance with the relevant school Acceptable Use Policy.

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 ICT / PHSCE 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
- 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 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
- 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 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:

- Letters, newsletters, web site
- Parents evenings
- Reference to the E-safety rules for parents

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 and Acceptable Use Policies
- The E-Safety Coordinator will receive regular updates through attendance of LEA / other training sessions and by reviewing guidance documents released by BECTA / YHGfL / LEA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The E-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 involved in ICT / 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 Governors Association / YHGfl 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 the school meets the e-safety technical requirements
- There will be regular reviews and audits of the safety and security of the school's 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 by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Coordinator
- All users in KS2 will be provided with a username and password by Arvato who will keep an up to date record of users and their usernames.
- All users in KS1 will be provided with a username by Arvato who will keep an up to date record of users and their usernames.
- 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.
- All 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 LEA is responsible filtering contract who maintain and supports the managed filtering service.
- In the event of the Filtering provider needing to switch off the filtering for any reason, or for any user/class, this must be logged and carried out by a process that is agreed by the LEA
- Any filtering issues should be reported immediately to East Riding on 01482 394444.
- Requests from staff for sites to be removed from the filtered list will be considered by the ICT support Rob Gutherless and Melanie Harbottle. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.

- An appropriate system is in place for users to report any actual / potential e-safety incident to their Teacher.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed system is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system.
- 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 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, 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, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT support can request to 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 these requests will be recorded and reviewed annually.
- 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 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. 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 particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of 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 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 checking software

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:

Also refer to Mobile Phone Acceptable Use Policy for pupils

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times - emergencies	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with 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 PDAs, PSPs		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 – School Spark – other sites not allowed	X							X
Use of social networking sites		X						X
Use of blogs – dependent on material eg. educational	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 and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the Esafety coordinator or Network technician – 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 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.

- Whole class or group email addresses will be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / Inappropriate Activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, 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, eg under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in UK
- pornography
- promotion of racial or religious hatred
- promotion of any kind of discrimination
- 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 Core IS/ERYC or the school
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- on-line gambling
- 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
- file Sharing from illegal sites

These activities are classed as acceptable but not during teaching / school hours.

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

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of 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 headteacher will be informed and this will be reported to the police.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

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: (However this does depend on severity and a teacher must use their judgement)

Action for misuse by pupils

1. Refer to class teacher
2. Refer to Headteacher / SLT / E-safety Coordinator / Technical Support
3. Inform Parents
4. Refer to the police

Sanctions for pupils

1. Warning
2. Removal of network / internet access rights for a stated length of time
3. Other Sanctions linked with behaviour policy eg. Pay Back / exclusion

Action for misuse by staff

1. Refer to line manager
2. Refer to Headteacher / SLT / E-safety Coordinator / ICT Technician
3. Refer to Local Authority
4. Refer to police

Sanctions for staff

1. Warning
2. An official warning
3. Suspension
4. Further disciplinary action

For examples of incidents of misuse please see Appendix 1

Appendix 1

Incidents of misuse by pupils

Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).
Unauthorised use of non-educational sites during lessons
Unauthorised use of mobile phone / digital camera / other handheld device
Unauthorised use of social networking / instant messaging / personal email
Unauthorised downloading or uploading of files
Allowing others to access school network by sharing username and passwords
Attempting to access or accessing the school network, using another student's / pupil's account
Attempting to access or accessing the school network, using the account of a member of staff
Corrupting or destroying the data of other users
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature
Continued infringements of the above, following previous warnings or sanctions
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
Using proxy sites or other means to subvert the school's filtering system
Accidentally accessing offensive or pornographic material and failing to report the incident
Deliberately accessing or trying to access offensive or pornographic material
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act

Incidents of misuse by staff:

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