BYLEY PRIMARY SCHOOL

E-Safety Policy

Approved by Governors: March 2018
Review Date: March 2019

Rationale

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology.

We have developed this e-safety policy to help to ensure safe and appropriate use. It applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

Technologies are an important learning tool but 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 this e-safety policy is to be used in conjunction with other school policies (e.g. behaviour, anti-bullying and child safeguarding 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.

The Education and Inspections Act 2006 empowers Head Teachers, 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.

Monitoring and Review of Policy

This e-safety policy has been developed in conjunction with:

- Head Teacher
- School's E-Safety Co-Ordinator
- Teachers
- Governors
- ICT technical staff
- Support staff
- Parent & Carers

Consultation has taken place through:

- Staff meetings
- Governors' meetings
- School website/Newsletters
- Parents' Consultation Evenings
- School Council
- INSET Days

This e-safety policy was approved by the *Governing Body*	March 2018
The implementation of this e-safety policy will be monitored by the:	*E-Safety Co-Ordinator & Headteacher*
Monitoring will take place at regular intervals:	*Once a year*
The *Governing Body/Governors 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:	*Once a year at a Governors Meeting*
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:	March 2019
Should serious e-safety incidents take place, the following external persons/ agencies should be informed:	*Cheshire West ICT Manager 01244 972126, CWaC Safeguarding Officer – Pam Beech 0151 356 5566 and Police – Karl Williamson (police e-safety)*

The school will monitor the impact of the policy using:

- *Logs of reported incidents (which is kept in Head Teacher's office)*
- *Feedback from staff and children*

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the e-safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.

The role of the e-safety Governor will include:

- *meeting when necessary with the designated e-safety Co-ordinator/s*
- *monitoring of e-safety incident logs*
- *reporting to relevant Governors' committee*

The e-safety Governor is: Mr Malcolm Such

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-ordinators
- The Head Teacher is responsible for ensuring that the e-safety Co-ordinators 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 will receive monitoring reports when necessary from the e-safety Co-ordinators
- The Head Teacher and 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(see appendix on dealing with e-safety incidents)

Designated e-safety Coordinator/s:

The Head Teacher and e-safety Coordinators:

- takes day to day responsibility for e-safety issues and have 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 (see appendix for e-safety incident log proforma)
- meet when necessary with e-safety Governor to discuss issues, review incident logs
- attends relevant meetings of Governors
- reports to Senior Leadership Team

The designated e-safety Coordinators are: Miss C Aldous and Mrs K Walsh

Technical staff:

ICT Technician/ICT Co-ordinators are responsible for ensuring:

- that the school's ICT infrastructure is as secure as possible and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements as advised by National Guidelines and Acceptable use policy

- 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/Learning Platform/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the e-safety Co-ordinator/Head Teacher 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 the school Acceptable Use Policy for staff (see appendix)
- they report any suspected misuse or problem to the e-safety Co-ordinator/Head Teacher/Senior Leader/ICT Co-ordinator/Class teacher/ for investigation/action/sanction
- digital communications with pupils (email/Learning Platform) 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 ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated persons for child safeguarding:

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 online contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

The designated persons for child safeguarding are: Head teacher, Mrs King, and Mr Such

Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil e-safety rules and acceptable use policy (see appendix)
- 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. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, Learning Platform and information about national/local e-safety campaigns/literature. Parents and carers will be responsible for:

- ensuring they are aware of the school's e-safety policy and rules
- endorsing (by signature) the Pupil Acceptable Use Policy
- accessing the school website

Teaching and Learning

Pupils

Children 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 is provided as part of ICT/PSHE/other lessons and regularly revisited – this covers both the use of ICT and new technologies in school and outside school
- Key e-safety messages are reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils are taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Pupils are helped to understand the need for the e-safety rules and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils are 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 are posted in all rooms
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Parents/carers

Parents and carers need to have a good understanding of e-safety risks and issues, as they play an essential role in the education of their children and in the monitoring/regulation of the children's online experiences. The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, learning platform
- Parents' evenings
- Reference to the Cheshire West website and other guidance from the LA

Education & Training – Staff

It is essential that all staff receive e-safety information and understand their responsibilities, as outlined in this policy.

All new staff will be made aware of the school's e-safety policy/rules as part of their induction programme, ensuring that they fully understand the Acceptable Use Policy

- The e-safety Coordinators will receive regular updates through attendance at LA/other information/training sessions and by reviewing guidance documents released by BECTA (whose documents will migrate to the DFE website in the coming months) Cheshire West 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 Coordinators will provide advice/guidance/training as required to individuals

Training – Governors

Governors will take part in e-safety training/awareness sessions, with particular importance for those who are members of any committee/group 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 or other relevant organisation
- Participation in school training/information sessions for staff or parents delivered at the school by LA or other professional teams

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.

- School ICT systems will be regularly updated to ensure up-to-date anti-virus definitions and Microsoft Windows Security Updates are installed. Essential software i.e. Acrobat Reader, Flash Player, Java, Internet Explorer, Smartboard etc. must be kept current
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling is securely located and physical access restricted
- All users have clearly defined access rights to school ICT systems
- All users are provided with a username and password to access the school network
- The "administrator" passwords for the school ICT system will be available to the Head Teacher and e-safety coordinators and kept in a secure place (school safe/HT office)
- School Data is securely managed when taken off the school site using encrypted memory devices or password protected files
- Users are 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 Cheshire West and Chester Council
- Any filtering issues should be reported immediately to Cheshire West's IT support
- Requests from staff for sites to be added or removed from the filtered list will be considered at the appropriate senior level
- An appropriate system is in place for users to report any actual/potential e-safety incident to the designated e-safety Co-ordinators (or other relevant person)
- 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
- ICT Support install new programmes on school workstations/portable devices

Internet

E-mail

- Pupils may only use approved e-mail accounts on the school system
- Pupils must tell a teacher immediately if they receive an offensive e-mail

- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone
- E-mail sent to an external organisation should be written carefully and authorised by a member of staff before sending
- The forwarding of chain letters is not permitted

Published Content and the school Learning Platform (VLE)

- The contact details on the Learning Platform should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published
- The Headteacher will take overall editorial responsibility and ensure the content is appropriate
- Members of staff will take overall editorial responsibility for their sections on the school's VLE and ensure that content is accurate and appropriate
- Parents will take responsibility for monitoring that their child's use of the school Learning Platform is appropriate
- Whilst the school will make every effort to ensure that content is kept as accurate and correct as possible, it recognises that inaccuracies will occasionally occur. In these circumstances the school will make every effort to correct any errors in as short a time frame as is possible.

Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs or pupil's work is published on the school website
- Pupil's full names will not be used anywhere on the VLE

Use of digital and video images - Photographic, Video

Staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. 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
- pupils must not take, use, share, publish or distribute images of others (obtained using school equipment) 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

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.

- e-safety will be taught regularly through a scheme of work with identified progression of knowledge, skills and understanding
- e-safety skills will be embedded through both discrete ICT and cross-curricular application
- In lessons where internet use is pre-planned, it is best practice that pupils are 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 visited
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that they can temporarily be removed from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- pupils will be taught to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

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 sensitive data using encryption and secure password protected devices

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				Students / Pupils			
Communication Technologies (outside of those available on the learning platform)	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓							✓
Use of mobile phones in lessons				✓ Emergency only				✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones or other camera devices			✓				✓	
Use of hand held devices e.g. netbooks, PDAs, PSPs, iPad, iPod	✓						✓	
Use of personal email addresses in school, or on school network		✓						✓
Use of school email for personal emails				✓				✓
Use of chat rooms/facilities				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites				✓				✓
Use of blogs		✓					✓	

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**				✓	✓
	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 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 WBC and/or the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	

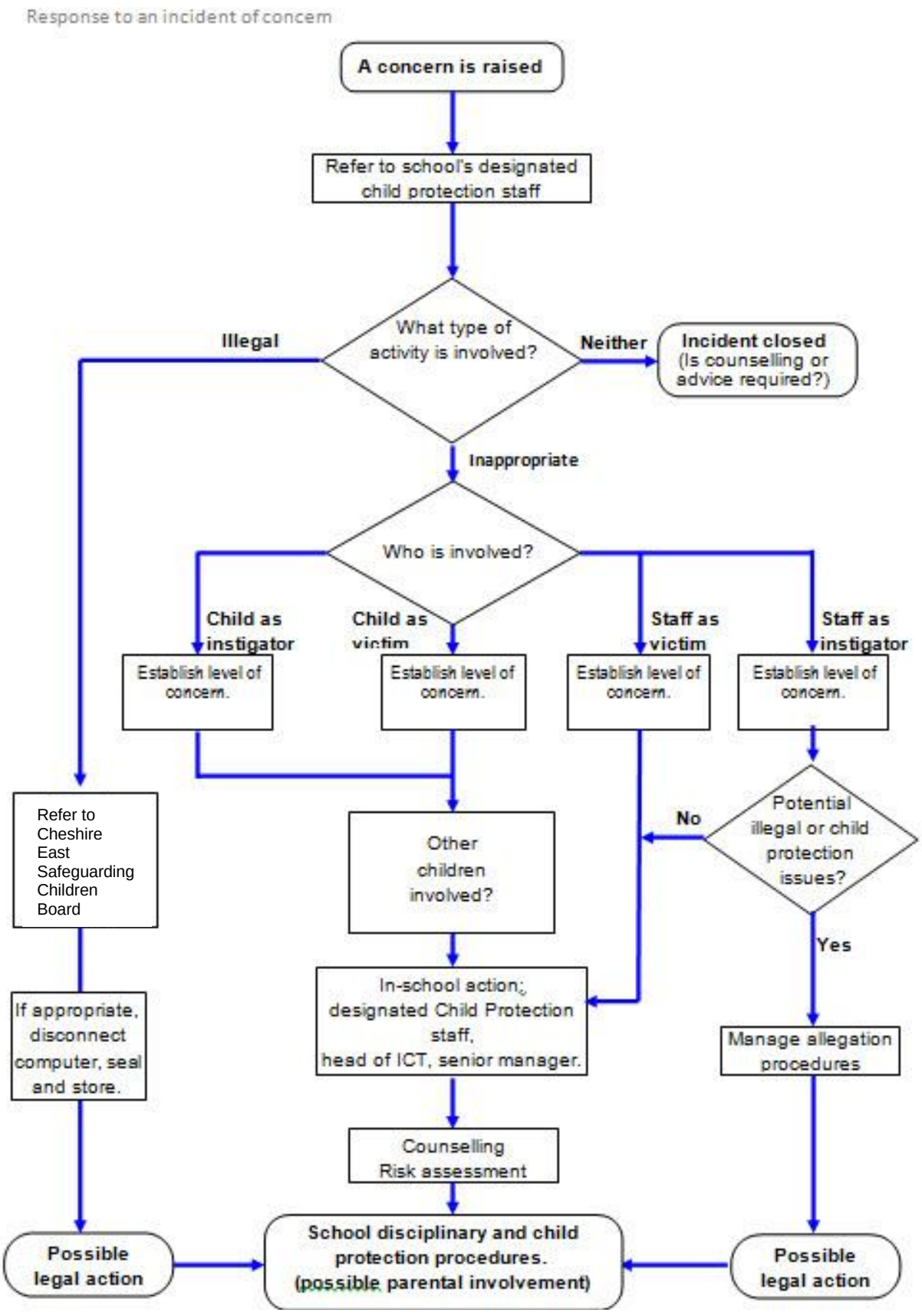
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				✓	
Creating or propagating computer viruses or other harmful files				✓	
Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet				✓	
Online gaming (educational)	✓				
Online gaming (non-educational)				✓	
Online gambling				✓	
Online shopping/commerce			✓ School purposes only		

File sharing			✓		
Use of social networking sites				✓	
Use of video broadcasting e.g. YouTube			✓		

Appendices

Appendix 1 - Responding to incidents of misuse

This flow chart should be consulted and actions followed accordingly.



N.B. Evidence will be saved/downloaded on HT's computer if necessary. Paper evidence or logs will be kept in HT's office

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 recommended that more than one member of staff is involved in 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:

Pupils **Actions/Sanctions**

Incidents:	Refer to class teacher/ tutor	Refer to Head of Department /Head of Year/other	Refer to Head Teacher	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 e.g. detention/exclusion (d) (e)
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			✓		✓	✓	✓	✓	✓ (d)
Attempting to access or accessing the school network, using the account of a member of staff			✓	✓	✓	✓	✓	✓	✓ (e)
Corrupting or destroying the data of other users			✓		✓	✓	✓	✓	✓ (d)
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			✓	✓	✓	✓	✓	✓	✓ (e)
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			✓	✓	✓	✓	✓	✓	✓ (e)
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			✓		✓			✓	

Staff **Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Head Teacher	Refer to Local Authority/ HR/Diocese	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).		✓	✓	possibly	✓	✓	possibly	possibly
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 e.g. holding or transferring data in an insecure manner	✓	✓				✓		
Deliberate actions to breach data protection or network security rules		✓	✓		✓	✓	possibly	possibly
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		✓	✓	possibly	✓	✓	possibly	Possibly
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		✓	✓			✓	possibly	Possibly
Using proxy sites or other means to subvert the school's filtering system		✓	✓		✓	✓	possibly	possibly
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		✓	✓			✓	possibly	possibly

E-Safety Audit

This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place.

Has the school an e-Safety Policy that complies with LA guidance?	**Y/N**
Date of latest update: March 2018	
The Policy was agreed by governors on: March 2018	
The Policy is available for staff at: Shared Area on network/ Staff Room	
And for parents at: School's Website	
The designated Child Safeguarding Teacher/Officer is: Mrs Kay Walsh (Headteacher)	
The e-Safety Coordinators are: Miss C Aldous & Mrs K Walsh	
Has e-safety training been provided for both pupils and staff?	**Y/N**
Are all staff made aware of the Acceptable Use Policy on appointment?	**Y/N**
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	**Y/N**
Have school e-Safety Rules been set for pupils?	**Y/N**
Are these Rules displayed in all rooms with computers?	**Y/N**
Internet access is provided by an approved educational Internet service provider and complies with DFE requirements for safe and secure access.	**Y/N**
Has the school filtering policy has been approved by SMT?	**Y/N**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Y/N**

Byley Primary School

E-Safety Rules

Think then Click...

These rules will keep us safe and help us be fair to others.

- I will only use the internet when an adult is with me
- I will not give out personal information or passwords
- I will tell an adult straight away if I come across any information or pictures that make me feel uncomfortable or that I am not sure about
- I will not use internet chat rooms
- I will not arrange to meet anyone I don't know
- I will not take or distribute images of anyone without their permission
- I understand that the school monitors my use of the ICT systems
- I will be a good online citizen and not do anything that hurts other people