Welburn Hall School

Headteacher: Mrs H Smith

E-Safety Policy

January 2014

Reviewed – no change Jan 15

Adopted by Governors:

Signed: **Date:**

This policy is reviewed annually by the Governing Body, however minor amendments may be made in the interim in response to developments in legislation, guidance, national policy or best practice. In such circumstances, the Governing Body will be informed by the E-safety Coordinator.

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 Headteachers, 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:

Governors:

Governors are responsible for approval of the E-Safety Policy and for reviewing its effectiveness. This will be carried out by the *relevant Committee* 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 committee 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 Coordinator.
- The Headteacher / Senior Leaders are 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 / 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 will receive regular monitoring reports from the E-Safety Coordinator.
- The Headteacher 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 Coordinator: *Niall Hayton*

- leads the e-safety committee
- 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, (through or with the assistance of the Network Manager).
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- meets regularly with the E-Safety Governor to discuss current issues, review incident logs.
- Ensure that the Headteacher is well-informed ahead of meetings of the Governing Body.
- reports regularly to the Senior Leadership Team.

Network Manager: *Catherine Barr*

The Network Manager 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.
- 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 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 Coordinator, Network Manager or Headteacher.
- 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
- students / pupils understand and follow the school e-safety and acceptable use policy
- students / pupils have as good as possible an 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 or activities where internet use is pre-planned students / 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 Senior Person for child protection: Niall Hayton

Must be aware/ made 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

E-Safety Committee

Members of the E-safety Committee will assist the E-Safety Coordinator with the production / review / monitoring of the school e-safety policy and guidance documents. They will also offer support in developing and presenting training materials and information to pupils/students, parents/carers and others.

Students / pupils:

Students/pupils are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they may be able to sign. In as much as it is possible, students/pupils should:

- have understanding of research skills and the need to uphold copyright regulations
- appreciate the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- 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.
- adopt 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 as much as they can the need to use the internet / mobile devices in an appropriate way. The school will therefore work to help parents understand these issues themselves. In many cases, parents and carers will be responsible for endorsing (by signature) the Student/Pupil Acceptable Use Policy.

Overview:

Education – students/pupils:

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students/pupils* to take a responsible approach. The education of *students/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/PHSE/other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Students/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.
- *Students / pupils should be helped to understand the need for the student/pupil Acceptable Use Policy, (AUP), and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.*
- *Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.*
- *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:

- Letters, newsletters, web site,
- Parents' evenings,
- Reference to online resources which may be of interest or value.

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. *It is expected that some staff will identify e-safety as a training need within the performance management process.*

- 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 training through respected resources such as EPICT.*

- *This E-Safety policy and its updates will be presented to and discussed by staff in staff/ team meetings/INSET days.*

- *The E-Safety Coordinator, or Network Manager, 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 of any sub-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.

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that its 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:

- The Network Manager will liaise with Schools ICT to ensure that its systems are managed in ways that aid the school in meeting the e-safety technical requirements outlined in the 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 by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).
- All users will be provided with a username and password by the Network Manager, who will keep an up to date record of users and their usernames. Users will be required to change their password at defined intervals.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and if the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.
- Schoosl ICT technical staff may monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- The Network Manager liaises with Schools ICT to ensure that 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.

Learning:

Welburn Hall School faces a particular challenge in educating students with learning difficulties and conditions such as Autistic Spectrum Disorder. This makes it especially important to ensure that teaching is done in an accessible and, where necessary, individualised way. Form Tutors will be expected to identify those students who require additional or different approaches to their learning.

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 or activities where internet use is pre-planned, it is best practice that students / 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 students / 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 Network Manager 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.
- Students / 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.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Welburn Hall's approach to the E- safety Curriculum:

There will be a half termly focus-in the second half Spring Term commencing with a collapsed curriculum on National Safer Internet Day which takes place every February. This may include making posters and leaflets, drama activities and making videos to promote e-safety. This will be followed by a weekly lesson for the next six weeks which will aim to develop the understanding of e-safety. This will be taught as part of the PSHE and citizenship curriculum and not as a discreet subject.

The areas to be covered include; the use of email, safe and appropriate use of the internet, chat and instant messaging, cyber bullying, social networking, mobile phones and mobile internet, file sharing, and most importantly who to talk to if they are worried about something that they have seen on line.

Why do we need to teach e-safety?

- To develop responsibility in children and young people's use of the Internet.
- To help children and young people develop the skills to use information wisely and well.
- To help children and young people avoid embarrassment or humiliation.
- To keep children and young people safe from predatory adults.
- To help children and young people avoid physical danger.
- To help children and young people avoid becoming victims of crimes such as identity theft and fraud.
- To help children and young people avoid harmful behaviours such as obsessive use of the Internet or digital games.

What will we teach?

KS2 children should be able to:

- Identify people who can help when using ICT and seek their help when appropriate.
- Understand that ICT can be used for fun, for learning and for communicating with others.
- Understand that some technologies should only be used when adults are present.
- Understand that Welburn Hall intranet is a safe place to share pictures and messages but that other places may not be safe.
- Understand that they can use technology to share information.

KS 3: children should be able to:

- Young people should recognise the need to knowwho it is they are sharing their learning with online.
- Understand the difference between different methods of communication (e.g. email, online forums).
- Know the difference between email and communication systems such as blogs and discussion forums.
- Know that websites sometimes include pop-ups that take them away from the main site and that these may be advertising.
- Know that bookmarking is a way to find safe sites again quickly.
- Begin to evaluate websites and know that not everything on the internet is true.
- Know that sometimes pictures and words on the Internet cannot be copied because they belong to somebody.

KS 3 KS4 and 5

Young people should be able to:

- Understand the need for rules to keep them safe when exchanging learning and ideas online.
- Recognise that information on websites may not be accurate or reliable and may be used for bias, manipulation or persuasion.
- Understand that the Internet contains fact, fiction and opinion and begin to distinguish between them.
- Understand the need to keep personal information and passwords private.
- Understand that if they make their personal information available online it may be seen and used by others.

KS4 and 5

Young people should be able to:

- Understand the safety issues related to communication tools including mobile phones, emails, instant messaging and social networking tools.
- Understand the potential dangers of using the Internet to communicate with people they do not know.
- Understand potential for misuse of personal data and the need to keep personal information private and to protect on-line identities and passwords.

- Understand some of the technical issues involved in efficient electronic communications, for example the need to protect wireless networks and to install firewalls and virus software.
- Know about some of the basic legal issues of using the internet, e.g. copyright and intellectual property legislation, the Computer Misuse Act (relating to hacking and unauthorised access to computing facilities), and data protection issues.
- Know the potential risks in shopping online and how to minimise them.
- Understand some of the health and safety issues involved in excessive use of computer games.

Use of digital and video images - Photographic, Video:

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students/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 students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students/pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students'/Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students/ pupils are published on the school website.
- Student's/Pupil's work can only be published with the permission of the student/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 device must be one provided by the school.
- 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 (below) once it has been transferred or its use is complete.

Personal devices and activities:

A wide range of rapidly developing communication technologies has the potential to enhance learning; however, there is a clear need to safeguard pupils/students in regard to personal devices. The following table sets out the particular limitations to their use determined by the school and this policy:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school		✔				✔		
Use of mobile phones in lessons				✔				✔
Use of mobile phones in social time		✔				✔		
Taking photos on mobile phones or other camera devices				✔				✔
Use of hand held devices eg PDAs, PSPs				✔				✔
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				✔				✔

Clarifications:

Adults:

For staff, the possession of mobile devices during working hours is subject to the following conditions:

- The device is not on their person during the course of their working time.
- The device is stored securely, eg. in a locker, locked drawer or locked room.
- 'Social time' for staff, (when they may use their mobile devices), refers to breaks, which should be taken in designated areas away from pupil/students.

For volunteers and visitors, the following must be made clear on their arrival:

- That, in general, they are not permitted to use their mobile phone, or any other recording device, on the premises. If they wish to make or receive a call, they should seek the agreement of school staff.
- That they must not take pictures, or make any other recordings without the express agreement of school staff.

Pupils/Students:

Day pupils bringing a mobile device to school:

- Must not attempt to conceal it.
- Must hand it to a member of staff on their arrival.
- May not, in usual circumstances, have it back until the end of the school day.
- Should agree beforehand any exceptions, (such as to aid learning), with a teacher or senior staff, who will ensure that the device is used appropriately and returned to a safe place afterwards.

Boarding pupils bringing a mobile device to school:

- Are subject to the same controls during the day as other pupils.
- May have use of their mobile device after tea.
- Must use it responsibly.
- Must report to a member of staff any problems or concerns regarding communications via that device.
- Should relinquish the device if a member of staff becomes concerned about its use on e-safety grounds.
- Must hand in the device before going to bed, for it to be kept safely.

College students bringing a mobile device:

- Are subject to the same controls during the day as pupils.
- May have use of their mobile device during the course of their time in the residential setting.
- Must use it responsibly.
- Must report to a member of staff any problems or concerns regarding communications via that device.
- Should relinquish the device if a member of staff becomes concerned about its use on e-safety grounds.

Note: the school acknowledges that some devices, such as iPads, are highly useful to some pupils/students; especially as a communication aid. It is accepted that, by agreement, arrangements can be made for these to be brought into school and college. However, parents/carers or other bodies should be asked to provide 'wi-fi only' models in such cases.

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 (eg by remote access).

- Users need to be aware that email communications may be monitored.

- Users must immediately report, to the E-safety Coordinator – 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, 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.

- 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:

The school believes that the activities referred to in the following section would be unacceptable 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. This 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, 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 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 SWGfL 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 (eg 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 (educational)			✔			
On-line gaming (non educational)					✔	

On-line gambling				✔	
On-line shopping / commerce		✔			
File sharing				✔	
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.

If any member of staff becomes aware of illegal activity on a computer, (either by seeing or suspecting that it is present), the E-Safety Coordinator and Network Manager must be informed. They should then work together to investigate and, in doing so, should consider the following list of response:

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,

it will be essential to preserve the evidence. In such cases, the computer should be disconnected from the mains immediately. It should not be shut down as this may erase evidence.

If the E-Safety Coordinator and Network Manager are convinced that the activity is illegal, (or strongly suspect that it is), they must contact the police.

If the E-Safety Coordinator and Network Manager have not seen illegal material, but suspect that it has been accessed/downloaded, the Network Manager should take advice/assistance from SICT regarding the viewing of activity logs. If, once the logs are seen, the Network Manager and E-Safety Coordinator are convinced that the material is illegal, they must contact the police.

If the material found is not illegal, but still considered inappropriate, the E-Safety Coordinator and Network Manager must:

1. Inform the Headteacher to enable them to determine the best course of action in regard to disciplinary procedures.
2. Ensure that advice and support is sought from NYCC.
3. Use the BECTA process, At Appendix 1, as guidance.

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 below.

Pupils/Students:

The following table identifies the range of actions or sanctions available to senior staff in regard to inappropriate acts by pupils/students:

Students / Pupils — Actions / Sanctions

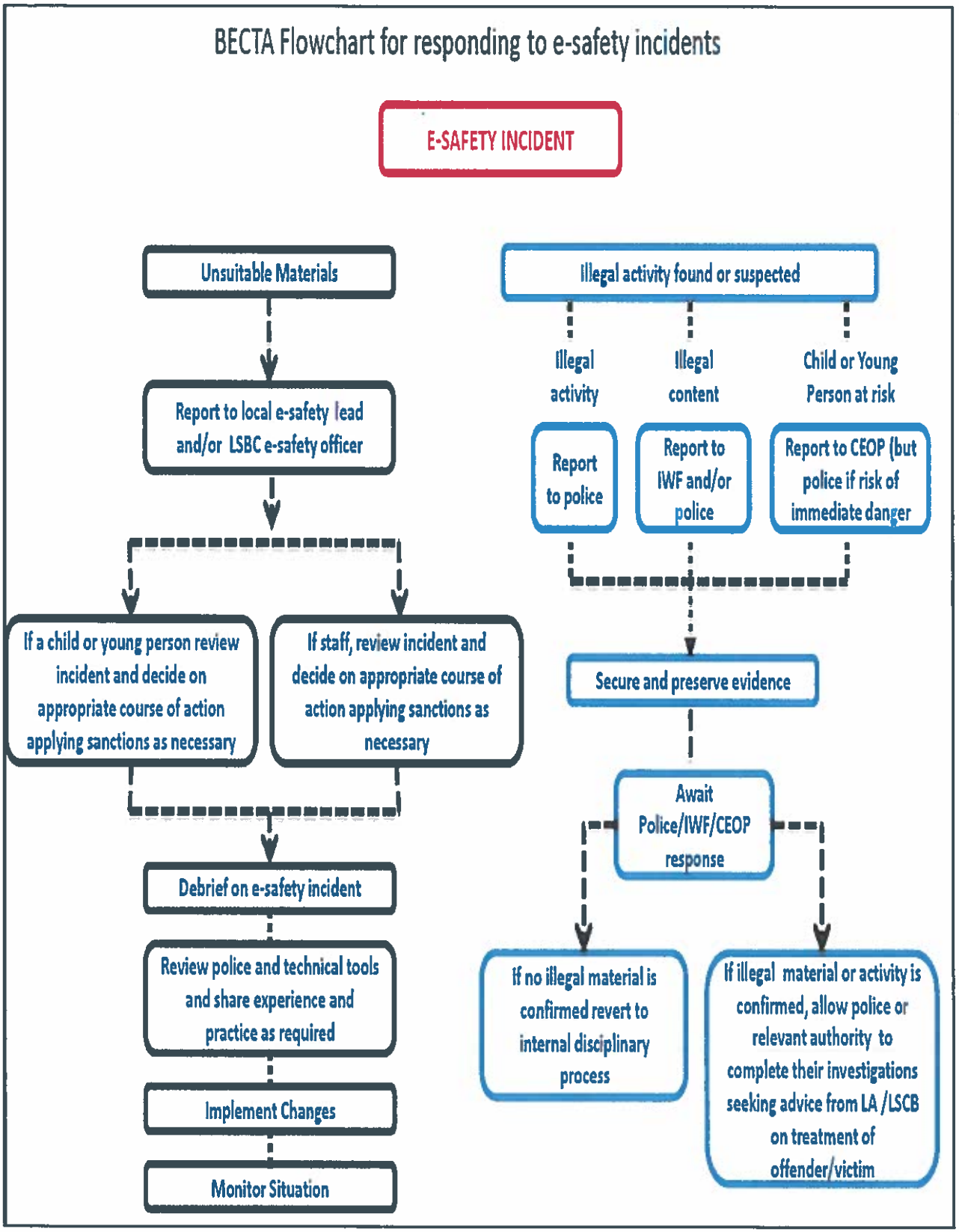
Incidents:	Refer to class teacher / tutor	Refer to Line Manager	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately 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 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			✔			✔	✔	✔	

Staff:

The following table identifies the range of actions or sanctions available to senior staff in regard to inappropriate acts by members of staff:

Staff	Actions / Sanctions							
Incidents:	Refer to line managerr	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal	✔	✔	✔	✔		✔		
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	✔	✔	✔			✔	✔	✔

Appendix 1


BECTA Flowchart for responding to e-safety incidents
E-SAFETY INCIDENT
Unsuitable Materials
Report to local e-safety lead and/or LSBC e-safety officer
If a child or young person review incident and decide on appropriate course of action applying sanctions as necessary
If staff, review incident and decide on appropriate course of action applying sanctions as necessary
Debrief on e-safety incident
Review police and technical tools and share experience and practice as required
Implement Changes
Monitor Situation
Illegal activity found or suspected
Illegal activity
Illegal content
Child or Young Person at risk
Report to police
Report to IWF and/or police
Report to CEOP (but police if risk of immediate danger
Secure and preserve evidence
Await Police/IWF/CEOP response
If no illegal material is confirmed revert to internal disciplinary process
If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations seeking advice from LA /LSCB on treatment of offender/victim