Windlesham School & Nursery

ICT & eSafety Policy

Last Reviewed: April 2018
Next Review Due: Spring Term, First Half, 2018/19

Key contacts:
eSafety Co-ordinator - Jane Waller
ICT Technician - Richard Ferries
ICT Teacher - Pam Moss

Windlesham School Trust Limited. Registered company no. 1172432 (England & Wales). Registered charity no. 269264. Registered office: 190 Dyke Road, Brighton, East Sussex, BN1 5AA

Contents

1 Development / Monitoring / Review of this Policy 1
2 Scope of the Policy 2
3 Roles and Responsibilities 2
3.1 Governors 2
3.2 Headteacher 2
3.3 eSafety Coordinator 2
3.4 ICT Technician and/or ICT Teacher 3
3.5 Teaching and Support Staff 3
3.6 Child Protection / Safeguarding Designated Teacher 3
3.7 eSafety Committee 4
3.8 Parents / Carers 4
4 Policy Statements 4
4.1 Education –pupils 4
4.2 Education – The Wider Community 5
4.3 Education & Training – Staff / Volunteers 5
4.4 Training – Governors 5
5 Technical – infrastructure / equipment, filtering and monitoring 5
6 Data Protection 7
7 Communications 8
8 Social Media - Protecting Professional Identity 9
9 Unsuitable / inappropriate activities 10
10 Responding to incidents of misuse 11
11 School Actions & Sanctions 13
Appendix 1 EYFS Policy for the use of cameras and mobile phones/ devices..... 16

1 Development / Monitoring / Review of this Policy

This eSafety Policy has been developed by a committee made up of:

- a member of the School's SMT
- The School's eSafety Coordinator
- Staff – including Teachers, Technical staff
- A School Governor

Schedule for Development / Monitoring / Review

This eSafety Policy was approved by the Governing Body on:	
Implementation of this eSafety Policy will be monitored by the:	*eSafety Committee*
Monitoring will take place at regular intervals:	*Annually*
The Governing Body will receive a report on the implementation of the eSafety Policy generated by the monitoring group (which will include anonymous details of eSafety incidents) at regular intervals:	*Annually*
The eSafety 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 eSafety or incidents that have taken place. The next anticipated review date will be:	*April 2018*
Should serious eSafety incidents take place, the following external persons / agencies should be informed:	Darrel Clews Safeguarding Team, Children's Services, BHCC. PC Vicky Jones Police Liaison Officer.

The school will monitor the impact of the Policy using:

- Logs of reported incidents
- Internal monitoring data for network activity

2 Scope of the Policy

This Policy applies to all members of the School community (including staff, pupils, volunteers, parents / carers, visitors) who have access to and are users of School ICT systems, both in and out of the 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 eSafety incidents covered by this Policy, which may take place outside of the School, but is linked to membership of the School. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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 eSafety behaviour that takes place out of School.

3 Roles and Responsibilities

The following section outlines the eSafety roles and responsibilities of individuals and groups within the School:

3.1 Governors

Governors are responsible for the approval of the eSafety Policy and for reviewing the effectiveness of the Policy. This will be carried out by the Governors receiving regular information about eSafety incidents and monitoring reports. A member of the Governing Body has taken on the role of eSafety Governor. The role of the eSafety Governor will include:

- Regular meetings with the eSafety Co-ordinator / Officer
- Regular monitoring of eSafety incident logs
- Reporting to relevant Governors/meetings

3.2 Headteacher

- The Headteacher has a duty of care to ensure the safety (including eSafety) of members of the School community, though the day to day responsibility for eSafety will be delegated to the eSafety Co-ordinator
- The Headteacher and (at least) another member of the Senior Management Team should be aware of the procedures to be followed in the event of a serious eSafety allegation being made against a member of staff. (see flow chart on dealing with eSafety incidents – included in section 11 – “Responding to incidents of misuse”).
- The Headteacher is responsible for ensuring that the eSafety Coordinator and other relevant staff receive suitable training to enable them to carry out their eSafety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal eSafety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Management Team will receive regular monitoring reports from the ESafety Co-ordinator.

3.3 eSafety Coordinator

- leads the eSafety committee
- takes day to day responsibility for eSafety issues and has a leading role in establishing and reviewing the school eSafety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an eSafety incident taking place.

- provides training and advice for staff
- liaises with the Local Authority / relevant bodies
- liaises with school technical staff
- receives reports of eSafety incidents and creates a log of incidents to inform future eSafety developments
- meets regularly with eSafety Governor to discuss current issues, review incident logs and filtering
- attends relevant meeting of Governors
- reports regularly to Senior Management Team

3.4 ICT Technician and/or ICT Teacher

The ICT Technician and/or ICT Teacher are responsible for ensuring:

- that the School's technical infrastructure is secure and is not open to misuse or malicious attack
- that the School meets required eSafety technical requirements
- that staff may only access the networks and devices through a properly enforced Password Protection Policy, in which passwords are regularly changed. Passwords are applied from Year 2 upwards.
- that they keep up to date with eSafety technical information in order to effectively carry out their eSafety role and to inform and update others as relevant
- that monitoring software / systems are implemented and updated as agreed in School policiesthat the use of the internet/email can be monitored in order that any misuse / attempted misuse can be reported to the eSafety Coordinator for investigation / action / sanction. A web filtering process is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.

3.5 Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of eSafety matters and of the current School eSafety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement
- they report any suspected misuse or problem to the eSafety Coordinator for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- eSafety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the principles of eSafety as summarised in the Pupil ICT Agreement
- pupils (depending on age) have an understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other School activities (where allowed) and implement current 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

3.6 Child Protection / Safeguarding Designated Teacher

should be trained in eSafety issues and be aware of the potential for serious child protection/safeguarding 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

3.7 eSafety Committee

The eSafety Committee provides a consultative group that has representation from the School community, with responsibility for issues regarding eSafety and monitoring the eSafety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the eSafety Committee will assist the eSafety Coordinator with:

- the production / review / monitoring of the School eSafety Policy / documents.
- mapping and reviewing the eSafety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs

  consulting stakeholders – including parents / carers about the eSafety provision

3.8 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, website and information about national / local eSafety campaigns / literature. Parents and carers will be encouraged to support the School in promoting good eSafety practice and to follow guidelines provided by the School.

4 Policy Statements

4.1 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 eSafety is therefore an essential part of the School's eSafety provision. Children need the help and support of the School to recognise and avoid eSafety risks and build their resilience.

Staff should reinforce eSafety messages across the curriculum. The eSafety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned eSafety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key eSafety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in research lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils (depending on age) should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the Pupil ICT Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices

- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the children visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be recorded on the eSafety incident log, with clear reasons for the need.

4.2 Education – The Wider Community

The School will provide opportunities for local community groups / members of the community to gain from the School's eSafety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and eSafety
- eSafety messages targeted towards grandparents and other relatives as well as parents.
- eSafety information for the wider community
- Supporting community groups eg Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their eSafety provision (possibly supporting the group in the use of Online Compass, an online safety self review tool - www.onlinecompass.org.uk)

4.3 Education & Training – Staff / Volunteers

It is essential that all staff receive eSafety training and understand their responsibilities, as outlined in this Policy. Training will be offered as follows:

- A planned programme of formal eSafety training will be made available to staff. This will be regularly updated and reinforced. An audit of the eSafety training needs of all staff will be carried out regularly.
- All new staff should receive eSafety training as part of their induction programme, ensuring that they fully understand the school eSafety Policy and Acceptable Use Agreements.
- The eSafety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This eSafety Policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The eSafety Coordinator will provide advice / guidance / training to individuals as required

4.4 Training – Governors

Governors should take part in eSafety training/awareness sessions via:

- Attendance at training provided by the Local Authority or other relevant organisation
- Participation in school training / information sessions for staff, parents or governors

5 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 eSafety responsibilities:

- School technical systems will be managed in ways that ensure that the School meets recommended technical requirements

- There will be regular reviews of the safety and security of School technical systems
- All users will have clearly defined access rights to School technical systems and devices.
- All users (at KS2 and above) will be provided with a username and password by the ICT Technician who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The “administrator” passwords for the School ICT system, used by the ICT Technician must also be available to the Bursar and kept in a secure place
- The ICT Technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licensing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users apart from office staff. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed Policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. **Personal data for the purposes of this Policy is any content that includes surname of Pupils Staff and Parents and Governors connected to the School currently, and/or connected to the School in the past.**

Bring Your Own Device (BYOD)

Windlesham School does not currently permit use of own devices on the School’s network.

Use of digital and video images

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, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry 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 (depending on age) 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.
- Parents/carers are asked not to take videos and digital images of their children at school events for their own personal use; the School arranges for professional copies to be available either for sale or on the School’s website.
- Staff and volunteers 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; personal equipment should not be used.

- 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 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.

6 Data Protection

Personal data (as defined in section 5) 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.

The School must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data

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 sensitive personal data is stored on any portable computer system, memory stick or removable media:

- the data must be password protected

- the device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected)
- the data must be securely deleted from the device, in line with School Policy once it has been transferred or its use is complete

7 Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the School currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults			Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
*Mobile phones may be brought to school		X		X				
**Use of mobile phones in lessons		X		X				
***Use of mobile phones in non-contact time		X		X				
Taking photos on mobile phones / cameras				X				
#Use of other mobile devices eg tablets, gaming devices		X					X	
##Use of personal email addresses in school, or on school network		X						
Use of school email for personal emails							X	
###Use of messaging apps		X						
Use of social media							X	
+Use of blogs		X					X	

*Mobile phones may be brought to school but kept in safe storage, in the staffroom or in a bag/drawer and not accessed in the presence of children.

**Mobile phones may be used for the purpose of teaching about the design of mobile apps or similar lesson. However, this will not be the teacher's personal mobile phone.

***Staff may use personal mobile phones during break times or times when children are not present in a safe location e.g. staffroom or empty classroom.

#Other mobile devices may only be used if appropriate for the lesson and if the device is the property of the school.

##Personal email addresses may be checked in school on the school network only at appropriate times – when children are not present and during staff breaks.

###Staff may access messaging apps during breaks in a secure environment ie staffroom or empty classroom.

+Staff may access blogs in lesson if appropriate to content of lesson, not on personal devices.

When using communication technologies the school considers the following as good practice:

- The official School email service may be regarded as safe and secure and is monitored. Staff should therefore use only the School email service to communicate with others when in School, or on School systems (eg by remote access).
- Users must immediately report, to the nominated person – in accordance with the School Policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- 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 social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while pupils at KS2 will be provided with individual ePals email addresses for educational use.
- Pupils should be taught about eSafety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the School website and only official email addresses should be used to identify members of staff.

8 Social Media - Protecting Professional Identity

The School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the School through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made on personal social media accounts to pupils, parents/carers or School staff
- They do not engage in online discussion on personal matters relating to members of the School community
- Personal opinions should not be attributed to the School
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The School's use of social media for professional purposes will be checked regularly by the eSafety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

9 Unsuitable / inappropriate activities

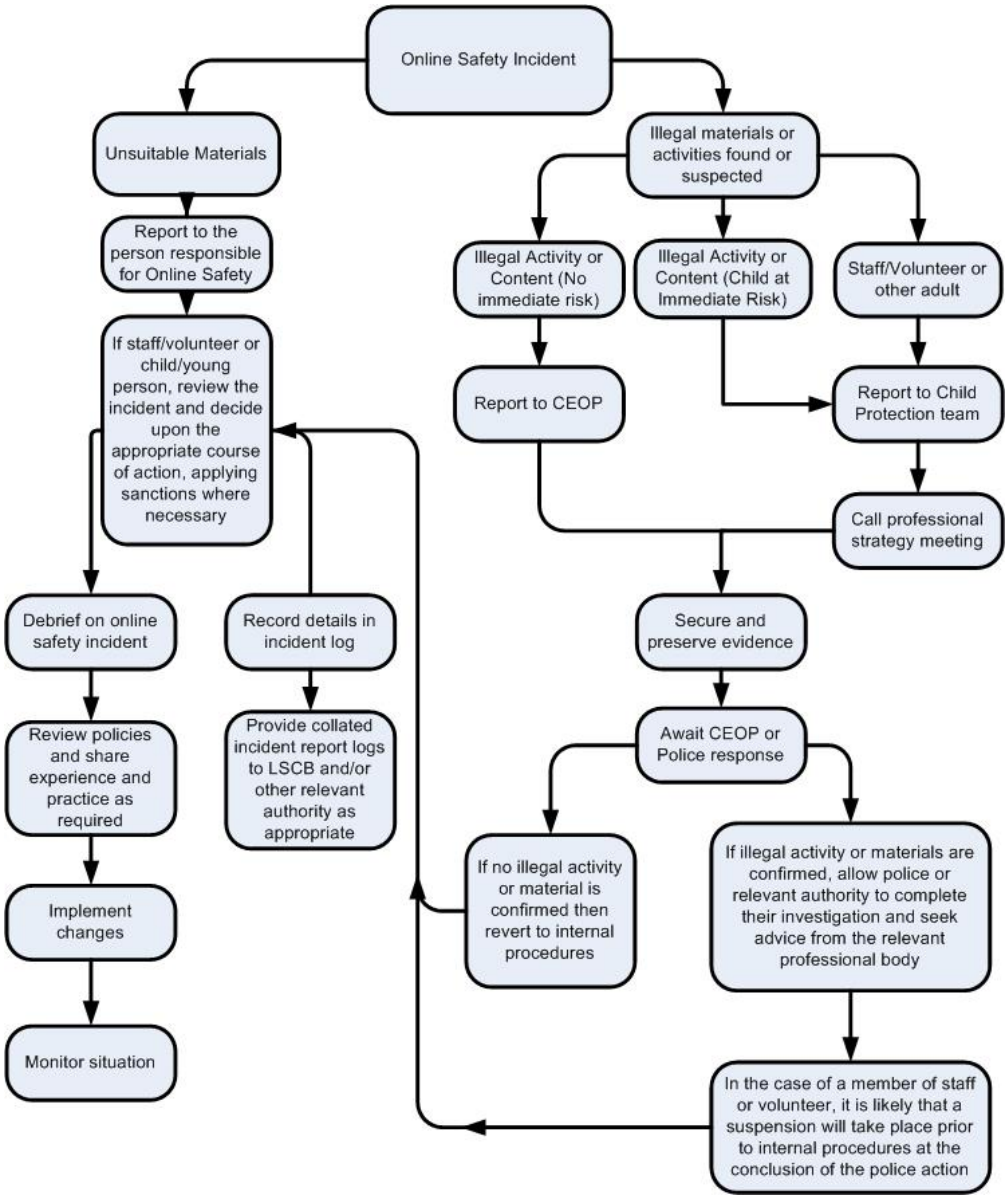
The School believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in School or outside School when using school equipment or systems. The School Policy restricts usage as follows:

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 –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the School					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce			X			
File sharing			X			
Use of social media			X			
Use of messaging apps			X			
Use of video broadcasting eg Youtube		X				

10 Responding to incidents of misuse

Illegal Incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the School community will be responsible users of digital technologies, who understand and follow School Policy. However, there may be times when infringements of the Policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the School and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

11 School Actions & Sanctions

It is more likely that the School will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, 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

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

Staff

Incidents:	Refer to eSafety Coordinator	Refer to Headteacher	Refer to Local Authority	Refer to Police	Refer to ICT Technician for action re filtering etc	Follow Disciplinary Procedure
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		x	x	x		x
Inappropriate personal use of the internet / social media / personal email	x					
Unauthorised downloading or uploading of files	x					
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	x					
Careless use of personal data eg holding or transferring data in an insecure manner	x					
Deliberate actions to breach data protection or network security rules	x	x			x	x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	x			x	x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x				x
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		x				x
Actions which could compromise the staff member's professional standing		x				
Actions which could bring the School into disrepute or breach the integrity of the ethos of the School		x				x
Using proxy sites or other means to subvert the School's filtering system	x	x				x
Accidentally accessing offensive or pornographic material and failing to report the incident		x				
Deliberately accessing or trying to access offensive or pornographic material		x				x
Breaching copyright or licensing regulations	x					
Continued infringements of the above, following previous warnings or sanctions		x				x

Appendix 1

EYFS Policy for the use of cameras and mobile phones/ devices

To ensure the safety and welfare of the children in our care, this policy outlines the protocols for the use of personal mobile phones/devices and cameras in the EYFS setting at Windlesham School.

Personal mobile phones, cameras and video recording equipment cannot be used when in the presence of children on school premises including the swimming pool.

· All mobile phones must be stored securely out of reach within the setting during contact time with children. This applies to staff, visitors, parents, volunteers and students.

· No parent is permitted to use their mobile phone or use its camera facility whilst inside school buildings, in the swimming pool or around the grounds when children are present.

· Mobile phones must not be used in any teaching area within the setting or within the bathroom area.

· In the case of a personal emergency, staff should use the school telephone. It is the responsibility of all staff to make families aware of the school telephone numbers.

· Personal calls may be made in non-contact time but not within the teaching areas.

· Personal mobiles, cameras or video recorders should not be used to record classroom activities. School equipment only should be used.

· Photographs and recordings can only be transferred to and stored on a school computer/IPad or laptop before printing.

· All telephone contact with parents and carers should be made on the school telephone.

· During group outings, nominated staff will have access to the school mobile which can be used in an emergency or for contact purposes. Staff may carry their own phones in bags but they should only be used in emergencies.

· In the case of school productions and sports day, parents and carers are permitted to take photographs/video footage of their own child in accordance with school protocols but we strongly advise against the publication of any such photographs on social networking sites. Most EYFS events will be videoed / photographed by school staff and then made available to parents