

Woodhouse Academy

E-Safety Policy

Reviewed: Summer 2017
Review Date: Summer 2019

The academy will ensure that:

- All systems are secure and not open to misuse
- Staff & pupils have up to date awareness of e-safety matters and rules to keep e-safe

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 academy will take every opportunity to help parents understand these issues and encourage them to support the academy in promoting good e-safety practice.

Parents / carers are requested to sign on the permission form in the planner to allow the school to take and use images of their children and for the parents / carers to agree.

Community Users

Community users who access school systems / website / VLE as part of the wider academy provision will be expected to sign a Community User AUP before being provided with access to school systems. These users will have limited access to school systems and be monitored by PCE software.

Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience, therefore allowing them to become responsible internet users.

Every pupils' planner contains the following good practice rules:

We use the school computers and internet connections for learning.

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

- I will ask permission before entering any web site, unless my teacher has already approved that site.
- On a network, I will use only my own login and password, which I will keep secret.
- I will not look at, change or delete other people's files.
- I will not bring DVDs or memory sticks to use in school without permission.
- I will only use the computers for school work and homework unless permission has otherwise been given.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- When sending e-mail, I will not give my home address or phone number, or arrange to meet someone.
- I will ask permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I will not use Internet chat.
- I will not use social network sites to make inappropriate comments about the school, pupils, or staff of the school.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I know that the school may check my computer files and may monitor the Internet sites I visit.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.

The school exercises its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Woodhouse Academy

E-Safety Policy

Reviewed: Summer 2017

Review Date: Summer 2019

Staff

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. School / academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the academy or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risks 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 in social media 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 academy or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

See also staff code of conduct.

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 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 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.
- In accordance with guidance from the Information Commissioner's Office, parent / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be

Woodhouse Academy

E-Safety Policy

Reviewed: Summer 2017

Review Date: Summer 2019

published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital /video images.

- 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, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Data Protection

See Data Protection Policy

Communication Technologies

Communication	Staff	Pupils
Mobile phones	Allowed in school, not to be used during lessons	Allowed in school, to be kept turned off in lockers
School devices such as tablets	Allowed	Allowed with staff permission
Own devices other than mobile phones	Allowed without pupil access	Kindles allowed
Use of personal email address in school or on school network	Allowed at certain times	Allowed with staff permission at certain times
Use of school email for personal emails	Not allowed	Not allowed
Use of messaging apps and social media on school network	Not allowed	Not allowed
Use of blogs	Allowed at certain times	Allowed at certain times
Use of streaming sites such a Youtube appropriate for age group and purpose	Allowed	Allowed at certain times with staff permission

Woodhouse Academy

E-Safety Policy

Reviewed: Summer 2017
Review Date: Summer 2019

Use of School Equipment / Systems in or Outside School

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & 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					
Using school systems to run a private business				x		
Using systems, applications, website or other mechanisms that bypass the filtering or other safeguards employed by the academy				x		
Infringing copyright				x		
Revealing or publicising confidential or propriety information (e.g. 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			

Woodhouse Academy

E-Safety Policy

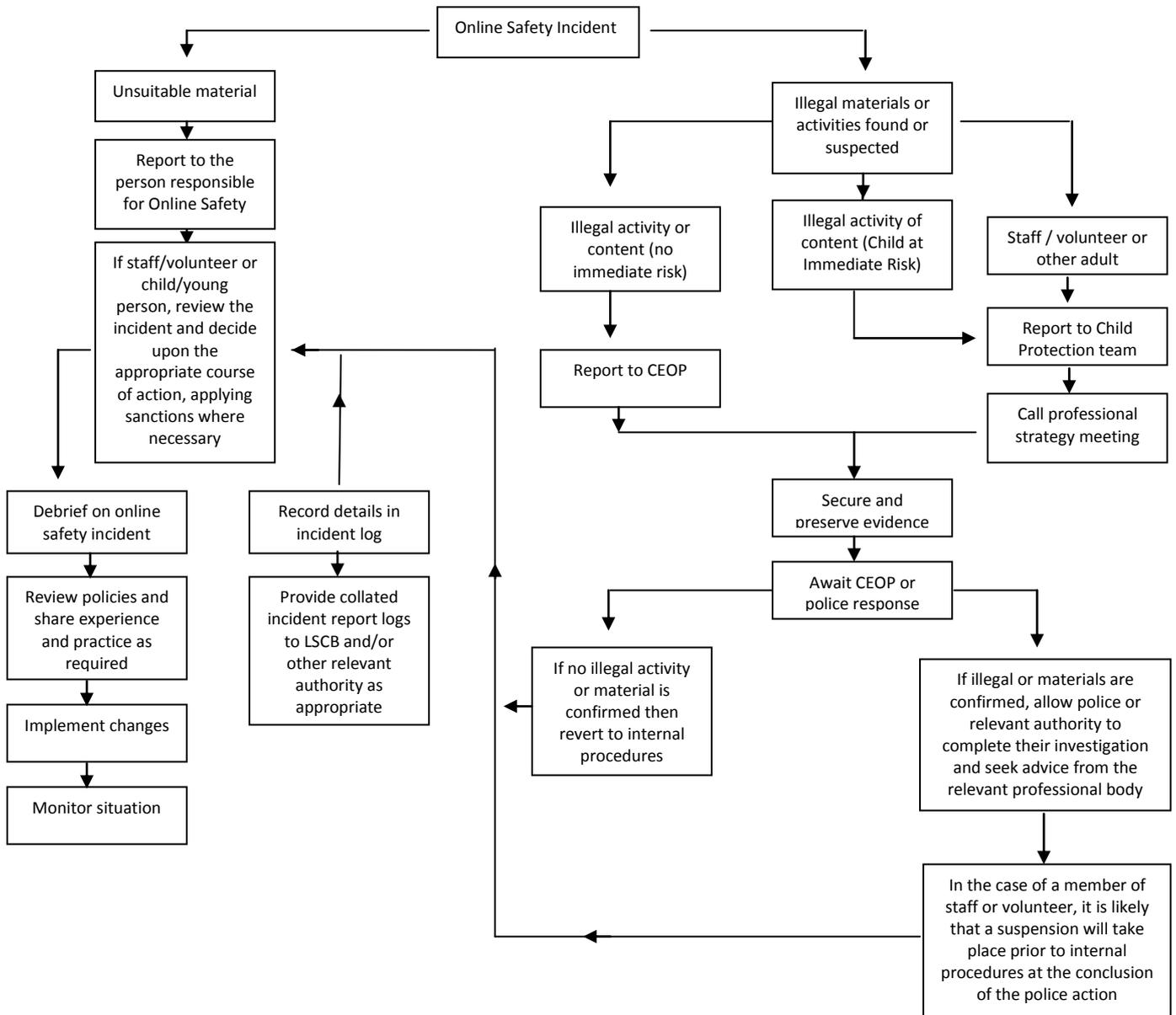
Reviewed: Summer 2017
Review Date: Summer 2019

Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of line services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see 'User Actions' above).

Illegal Incidents

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



Investigations will be undertaken using standard safeguarding procedures.

Woodhouse Academy

E-Safety Policy

Reviewed: Summer 2017

Review Date: Summer 2019

Pupils

Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Principal	Refer to Policy	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. payback / exclusion
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		X
Unauthorised use of non-educational sites during lessons	X								
Unauthorised use of mobile phone / digital camera / other mobile device	X	X							
Unauthorised use of social media / messaging apps / personal email	X				X		X		X
Unauthorised downloading or uploading of files	X				X			X	
Allowing others to access academy network by sharing username and passwords	X							X	
Attempting to access or accessing the academy network, using another student's / pupil's account	X							X	
Attempting to access or accessing the academy network, using the account of a member of staff	X	X			X	X	X		X
Corrupting or destroying the data of other users	X	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			X
Continued infringements of the above, following previous warnings or sanctions	X	X			X	X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X		X	X	X		X
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X	X		X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X							X	
Deliberately accessing or trying to access offensive or pornographic material	X	X			X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X			X	X			X

Woodhouse Academy

E-Safety Policy

Reviewed: Summer 2017
Review Date: Summer 2019

Staff

Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher / Principal	Refer to Local Authority / HR	Refer to police	Refer to technical support staff 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)	X	X	X	X	X			X
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X	X				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	X				X		
Careless use of personal data e.g. holding or transferring data in a insecure manner	X	X				X		
Deliberate actions to breach data protection or network security rules	X	X	X		X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware software	X	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			X
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils	X	X	X		X			X
Actions which could compromise the staff member's professional standing	X	X			X	X		
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy	X	X			X	X		
Using proxy sites or other means to subvert the school's / academy's filtering system	X	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		X			X
Breaching copyright or licensing regulations	X	X			X			X
Continued infringements of the above, following previous warnings or sanctions	X	X	X		X			X