 <p>North Wootton Academy</p>	<p>North Wootton Academy Priory Lane North Wootton Kings Lynn Norfolk PE30 3PT</p>
<p>Name of policy:</p>	<p>Online Safety</p>
<p>Lead member of staff with responsibility for this policy:</p>	<p>Craig Blackmur</p>
<p>Date of governors meeting when policy agreed:</p>	<p>March 2020</p>
<p>Type of governors meeting:</p>	<p>Academy Council</p>
<p>Date of implementation:</p>	<p>March 2020</p>
<p>Details of dissemination:</p>	<p>This policy is available on our school website and is available on request from the school office.</p>
<p>Frequency for review:</p>	<p>Annually</p>



Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by the Computing and E-safety lead and the DSL made up of:

- Principal / Senior Leaders
- Online Safety Co-ordinator
- Staff – including Teachers and Technical staff
- Governors

Consultation with the whole academy community has taken place through a range of formal and informal meetings.



Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governors on:	
The implementation of this Online Safety policy will be monitored by the:	DSL Online Safety Co-ordinator
Monitoring will take place at regular intervals:	Half-termly
The Board of Directors / Governing Body / Governors Sub Committee will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	When incidents occur
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2021
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Alan Evans (EMAT) Claire Smith (Academy Council) Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
 - students / pupils
 - parents / carers
 - staff

Scope of the Policy

This policy applies to all members of the academy community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of academy digital technology systems, both in and out of the academy.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy. 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 academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents if inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the academy.

Governors / Board of Directors

Governors / Directors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Board has taken on the role of Safe Guarding Governor. The role of the Governor will include:

- meetings with the Online Safety Co-ordinator
- attendance at Online Safety meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors.

Principal and Senior Leaders

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The Principal and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Principal / Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal / 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 online 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 / Senior Management Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the EMAT
- liaises with Academy technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,

- meets with Safe Guarding Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings
- reports regularly to Senior Leadership Team

Network Manager / Technical staff

The Network Manager / Technical Staff / Co-ordinator for ICT / Computing is responsible for ensuring:

- that the academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the academy meets required online safety technical requirements and EMAT guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal / Senior Leader; Online Safety Office for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in academy policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current academy Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Principal / Senior Leaders; Online Safety Officer for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the Online Safety Policy and acceptable use policies
- students / pupils have a good 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 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 Safeguarding Lead

Should be trained in Online Safety 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
- online-bullying

Students / Pupils:

- are responsible for using the academy digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the academy's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the academy in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / Learning Platform and on-line student / pupil records
- their children's personal devices in the academy (where this is allowed)

Policy Statements

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 online safety / digital literacy is therefore an essential part of the academy's online safety provision. Children and young people need the help and support of the academy to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online 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 taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. [N.b. additional duties for schools / academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.](#)
- Students / pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside academy.
- 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 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, staff should be vigilant in monitoring the content of the websites the young people visit.

In light of the new framework released by the Department for Education (<https://www.gov.uk/government/publications/teaching-online-safety-in-schools>) additional changes will be made to the provision of online safety within the academy. The guidance outlines several new topics which will be integrated into our curriculum. Within the section 'How to navigate the internet and manage information' the guidelines state that the children should

be taught about: Password phishing; the use of cookies; GDPR and Privacy settings. These topics will all be taught within a unit educating children on the use of social media. This unit will also encompass topics in other areas of the new guidance: 'Wellbeing and the impact on confidence' - image filters; digital enhancement and the role of influencers on social media and 'How to stay safe online' – content which incites.

Within the 'Wellbeing' section of the new guidance, the impact of time spent online and its link to mental health is another topic which is not currently taught as part of our Online Safety provision. This will therefore be integrated into our PHSE curriculum at the beginning of the academic year. As part of the academy SRE and PHSE curriculum, peer-pressure is a focus area and therefore the following topics from the new guidance will become part of that curriculum: Live Streaming and Online Challenges.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online 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 online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The academy will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, Learning Platform
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

Education & Training – Staff / Volunteers

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the academy Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Lead will provide advice / guidance / training to individuals as required.

Training – Governors / Directors

Governors / Directors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the MAT
- Participation in academy training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The academy will be responsible for ensuring that the academy 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 online safety responsibilities

- Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of academy technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to academy technical systems and devices.
- Lee Nicholls 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
- **Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. N.b. additional duties for schools / academies under the Counter Terrorism and Securities Act 2015 which requires schools / academies to ensure that children are safe from terrorist and extremist material on the internet. (see appendix for information on “appropriate filtering”).**
- Academy 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.

Use of digital and video images

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, parents / carers and students / 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 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 e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at academy 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 published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy 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 academy 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.
- Student’s / Pupil’s work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK change following the European Union General Data Protection Regulation (GDPR) [announced in 2016](#). As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data.

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

- 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.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.

- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of 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 personal data is stored on any portable computer system, memory stick or any other removable media:


- The data must be encrypted and password protected.
- The device must 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 academy policy once it has been transferred or its use is complete.

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school / academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school /academy context, either because of the age of the users or the nature of those activities.

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

	Ac ce pt ab le	Ac ce pt ab le	Ac ce pt ab le	U na cc ep ta bl e	U na cc ep ta bl e an d ill eg al
User Actions					
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:					X
					X

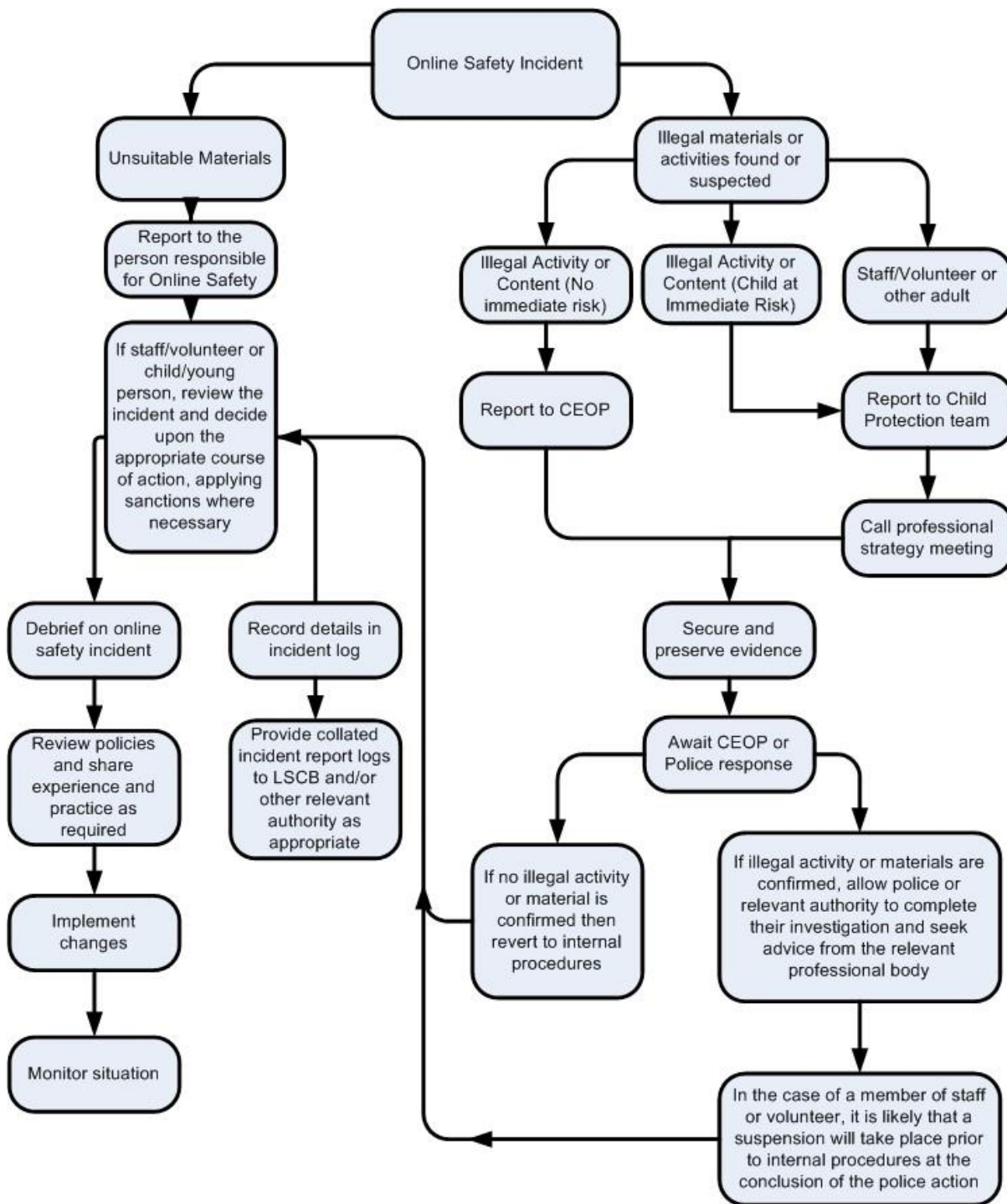
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to 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	
Promotion of extremism or terrorism				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 / academy				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 e.g. Youtube		X			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online 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 web site(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 and appendix) for responding to online safety incidents and report immediately to the police.



School / Academy Actions & Sanctions

It is more likely that the academy 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:

Actions / Sanctions									
Students / Pupils Incidents	Refer to class teacher / tutor	Refer to Head of Department / Year / other	Refer Headteacher / Principal	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 (see list in earlier section on unsuitable / inappropriate activities)		X	X	X		X			
Unauthorised use of non-educational sites during lessons	X							X	
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X					X		X	
Unauthorised / inappropriate use of social media / messaging apps / personal email	X					X			
Unauthorised downloading or uploading of files	X		X		X				X
Allowing others to access school / academy network by sharing username and passwords			X			X	X		

Attempting to access or accessing the school / academy network, using another student's / pupil's account			X			X	X		
Attempting to access or accessing the school / academy network, using the account of a member of staff			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	
Continued infringements of the above, following previous warnings or sanctions			X			X	X		
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school			X			X	X		
Using proxy sites or other means to subvert the school's / academy's filtering system		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
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X							X	

Actions / Sanctions

Staff Incidents	Refer to line manager	Refer to Principal	Refer to Local Authority / HR	Refer to Police	Refer to Data Protection Officer	Refer to Trust		
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		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				X		
Careless use of personal data e.g. holding or transferring data in an insecure manner		X				X		
Deliberate actions to breach data protection or network security rules		X				X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		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 students / pupils		X	X					
Actions which could compromise the staff member's professional standing		X	X					
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		X	X					
Using proxy sites or other means to subvert the school's / academy's filtering system		X	X		X			
Accidentally accessing offensive or pornographic		X						

material and failing to report the incident								
Deliberately accessing or trying to access offensive or pornographic material		X	X					
Breaching copyright or licensing regulations		X	X					
Continued infringements of the above, following previous warnings or sanctions		X	X					



Home Learning Arrangements

During the current national pandemic there is the possibility the learning will transition from school to home again. If this occurs then all communication between members of staff and pupils will take place over Academy monitored systems (nsix) allowing the DSL to safeguard and monitor conversations. Communication between members of staff and pupils should only take place under the following circumstances:

- Whilst using the provided nsix account for both staff and pupils
- For the purpose of providing educational resources or feedback
- Between the hours of 8:30-15:30
- For the purpose of welfare checks

If for any reason not listed above, communication needs to be had with a child or parent, staff should seek guidance and approval from DSL.

Whilst communicating with a pupil staff should ensure the following:

- Personal conversations are not taking place unless necessary for the welfare of the child.
- Teaching standards must always be adhered to.
- Images/videos should not depict members of staff or inappropriate backgrounds.

Acknowledgements

North Wootton Academy would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy:

- Members of the SWGfL Online Safety Group
- 360 degree safe Online Safety Self Review Tool