WIDNES ACADEMY

ASPIRING AND ACHIEVING

Online Safety Policy

Ratified by Governors: Spring 2026

Next Review Date: Spring 2027

Link: Mrs L.kirchin

A GREAT PLACE **TO BE A PART OF**

MEMBER OF THE WADE DEACON TRUST

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity (Trust Based)

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

The Education and Inspections Act 2006 empowers Headteachers/Principals/Head of School to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the Widnes 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 school but is linked to membership of Widnes Academy.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Widnes 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 of 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 Widnes Academy

Governors

The Local Governing Body 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 has taken on the role of Online Safety Governor as part of the wider remit of Safeguarding Governor

The role of the Online Safety Governor will include:

• regular meetings with the Safeguarding Lead

• regular monitoring of online safety incident logs

• reporting termly to Governing Body meetings

Principal and Senior Leaders

• The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community.

• The Principal and (at least) another member of the Senior Leadership 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 and Senior Leaders are responsible for ensuring that relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

• The Principal and 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 school/academy will need to describe this and may wish to involve the Local Authority/MAT/other responsible body in this process)

Online Safety Lead Laura Kirchin (liaises with the Safeguarding Team)

• 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 Local Authority/MAT/relevant body

• liaises with Trust technical staff

• receives reports of online safety incidents (on CPOMS) and creates a log of incidents to inform future online safety developments

, • meets regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering/change control logs

• reports regularly to Senior Leadership Team

Network Manager/Technical staff

The technical support for the school is managed by Wade Deacon Trust overseen by the ICT manager

Those with technical responsibilities are 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 any Local Authority/MAT/other relevant body online safety policy/guidance that may apply.

• that users may only access the networks and devices through a properly enforced password protection policy

• 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 networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Principal and Senior Leaders; Online Safety Lead 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 school/academy online safety policy and practices including GDPR protocols.

• they have read, understood and signed the staff acceptable use policy/agreement

• they report any suspected misuse or problem to the Principal for investigation and action

• 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

• pupils understand and follow the Online Safety Policy and acceptable use policies

• 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

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

Pupils:

All Pupils who bring devises into school must switch them off before entering the building and hand them to their class teacher who will store them and hand them out to the children as they are leaving the building. Devices are not to be turned on until leaving the school premises. Any children who attend an after school club will have their mobile handed to the school office by their teacher and they can collect on leaving the building after the club finishes.

• are responsible for using the academy digital technology systems in accordance with the pupil acceptable use agreement

• 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, social media 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 school/academy (where this is allowed)

Policy Statements 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 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 school 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 are provided as part of Computing/PHSE/other lessons and are regularly revisited

• Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities

• Pupils will 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.

• Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

• Pupils will 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.

• Pupils will be helped to understand the need for the 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 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 are 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 (e.g. racism, drugs, 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 auditable, with clear reasons for the need

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:

- Curriculum activities
- Letters, newsletters, web site, social media
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day

Education – The Wider Community

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

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The academy website will provide online safety information for the wider community
- Sharing their online safety expertise/good practice with other local schools
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their online safety provision

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 via The National College and through Safeguarding training updates. 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 school/academy online safety policy and acceptable use agreements.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Training – Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any 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 Local Authority/MAT/National Governors Association/or other relevant organisation

• Participation in academy training/information sessions for staff or parents

Technical – infrastructure/equipment, filtering and monitoring

The academy, with support from the Wade Deacon Trust, 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:

Widnes 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 school/academy technical systems

• Servers, wireless systems and cabling is securely located and physical access restricted

• All users will have clearly defined access rights to school/academy technical systems and devices.

• All users (at KS2 and above) will be provided with a username and secure password by the school IT technician who will keep an up to date record of users and their usernames. Each class teacher will be responsible for the security of their class username and passwords with children at KS2 being encouraged to be responsible for their own.

• The "master/administrator" passwords for the academy systems, used by the Network Manager (or other person) must also be available Principal or other nominated senior leader and kept in a secure place (e.g. school/academy safe)

• Graham Davies, as the IT technician allocated to the school by Wade Deacon Trust 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 access is filtered for all users. 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. There is a clear process in place to deal with requests for filtering changes (see appendix for more details)

• Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet

. • The academy has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc)

• Widnes Academy technical staff, in liaison with Wade Deacon Trust 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 via Wade Deacon Trust 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 devices are protected by up to date virus software.

• An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. This involves a separate login which is provided by school and which restricts access to any sensitive documents or material. Access to the schools MIS system is overseen by the class teacher. No passwords are to be shared.

• An agreed policy is in place – via the Wade Deacon Trust - regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school.

• An agreed system is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.

An agreed policy is in place – Wade Deacon Trust Code of Conduct - regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies will be an integral part of the school's online safety education programme.

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 pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying 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.

• 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 in 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 pupils are appropriately dressed and are not participating in activities that might bring the individuals or the academy 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 anywhere on a website or blog, particularly in association with photographs.

• Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data. More detailed guidance is available in the appendices to this document.

Widnes Academy, as part of the Wade Deacon Trust, follows all the policies and procedures agreed by the Trust including:

• Data Protection Policy

• Acceptable Use of the Internet for Parents and Carers

• Freedom of Information Publication Scheme

• Data Privacy Statements

• Information Communication Systems Policy

• Social Media Policy • Safeguarding Policy

The above named policies can be found on the school website at www.widnesacademy.co.uk

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies, the academy considers the following as good practice:

- The official Widnes Academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the academy email service to communicate with others when in school, or on school/academy systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the academy 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, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official

(monitored) /academy 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 and above will be provided with individual school/academy email addresses for educational use.
- Pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They are also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

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 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 an academy context, either because of the age of the users or the nature of those activities.

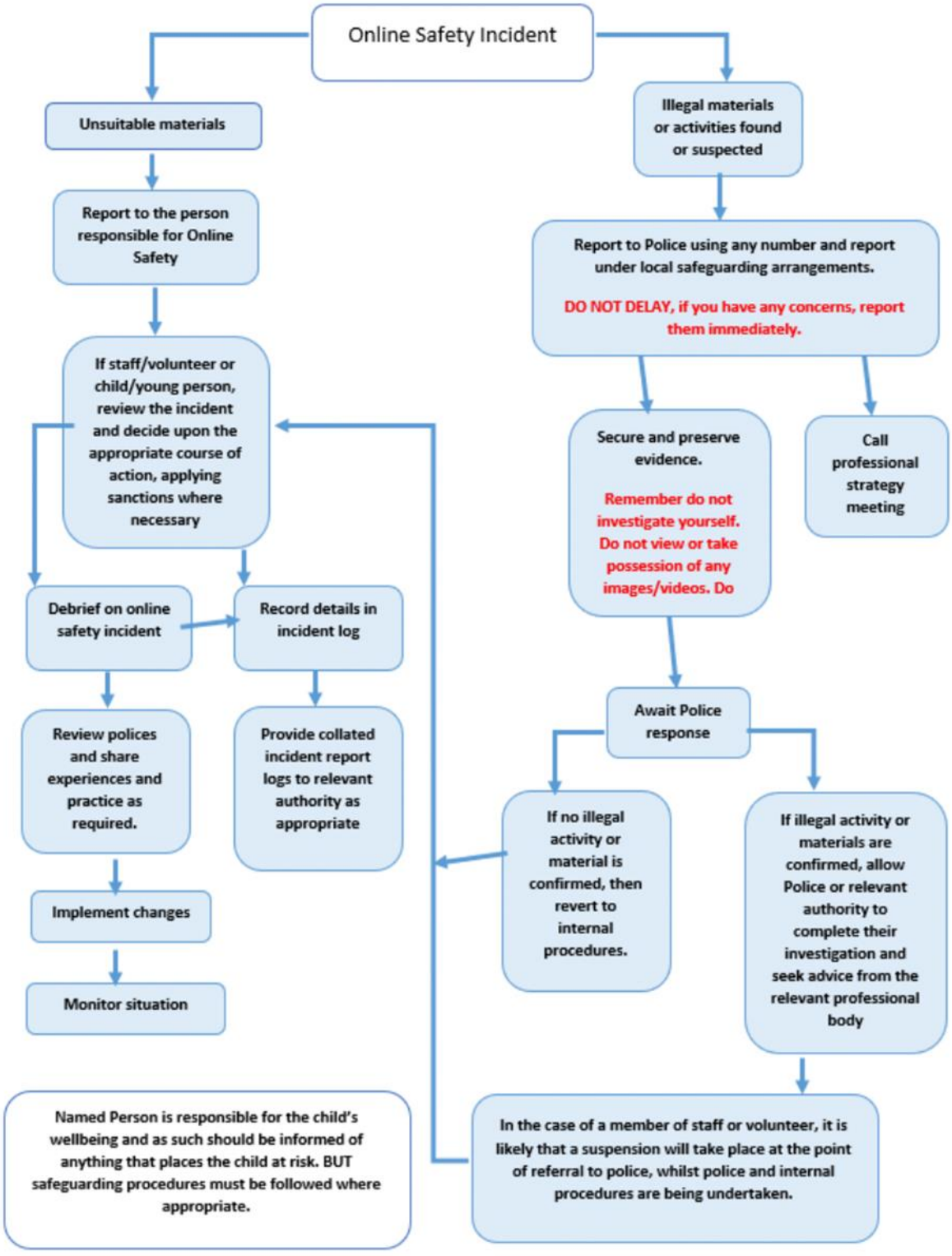
The academy believes that the activities referred to in the following section would be inappropriate in a academy context and that users, as defined below, should not engage in these activities in/or outside the school/academy when using academy equipment or systems.

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated user	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 N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					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	
	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	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)						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 (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				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).


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Other Incidents

It is hoped that all members of the Widnes Academy community will be responsible users of digital technologies, who understand and follow academy 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: o Internal response or discipline procedures o Involvement by Local Authority/Academy Group or national/local organisation (as relevant). o 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:

o incidents of 'grooming' behaviour o the sending of obscene materials to a child o adult material which potentially breaches the Obscene Publications Act

o criminally racist material o promotion of terrorism or extremism

o offences under the Computer Misuse Act (see User Actions chart above)

o 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/academy and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes.

The completed form should be retained by the group for evidence and reference purposes.

Widnes 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:

Students/Pupils Incidents	Refer to class teacher/tutor	Refer to Head of Department/Year/other	Refer to 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 e.g. 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					
Unauthorised use of non-educational sites during lessons									
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device									
Unauthorised/inappropriate use of social media/ messaging apps/personal email									
Unauthorised downloading or uploading of files									
Allowing others to access school/academy network by sharing username and passwords									
Attempting to access or accessing the school/academy network, using another student's/pupil's account									
Attempting to access or accessing the school/academy network, using the account of a member of staff									
Corrupting or destroying the data of other users									
Sending an email, text or 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/academy into disrepute or breach the integrity of the ethos of the school									
Using proxy sites or other means to subvert the school's/academy'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 Incidents	Actions/Sanctions							
	Refer to line manager	Refer to Headteacher Principal	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 (see list in earlier section on unsuitable/inappropriate activities).		X	X	X				
Inappropriate personal use of the internet/social media/personal email								
Unauthorised downloading or uploading of files								
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account								
Careless use of personal data e.g. holding or transferring data in an insecure manner								
Deliberate actions to breach data protection or network security rules								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software								
Sending an email, text or 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/academy into disrepute or breach the integrity of the ethos of the school/academy								

Using proxy sites or other means to subvert the school's/academy'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								