Wadham School

Online Safety Policy

DRAFT

Who is Responsible?	Governing Body
Statutory Policy?	Yes
Review Timescale	Every year
Approval Date	
Next Review	

Signed ..... Date: .....

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school esafety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students / pupils themselves. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students 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 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 the school/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 *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 online safety behaviour that take place out of school.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

• Access to illegal, harmful or inappropriate images or other content

• Unauthorised access to / loss of / sharing of personal information

• The risk of being subject to grooming by those with whom they make contact on the internet.

• The sharing / distribution of personal images without an individual's consent or knowledge

• Inappropriate communication / contact with others, including strangers

DRAFT

• Cyber-bullying

• Access to unsuitable video / internet games

• An inability to evaluate the quality, accuracy and relevance of information on the interne

t • Plagiarism and copyright infringement

• Illegal downloading of music or video files

• The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, antibullying and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students'resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while 3 using the internet and other communications technologies for educational, personal and recreational use.

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. Cyber-bullying, or other e-safety incidents are covered by this policy. These sometimes take place out of school, but are linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

Governors

Governors 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 Body* has taken on the role of *Online Safety Governor* The role of the Online Safety *Governor/* will include:

- regular meetings with the Online Safety Co-ordinator/DSL

DRAFT

- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors meeting
- Governors should take part in e-safety training.

Headteacher and Senior Leaders:

The *Headteacher* 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 Headteacher and senior leaders are responsible for ensuring that this policy and the various Acceptable Use Policies are consistent and appropriate to deliver the required level of e-safety

• The Headteacher and senior leaders are responsible for taking appropriate disciplinary action in case of breach of these policies

- The Headteacher and the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against <u>any member of the school community and certainly against a student.</u>
- *The Headteacher and 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 Headteacher 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 Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.*

Network Manager / Technical staff:

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

• that the school's ICT infrastructure is secure and is not open to misuse or malicious attack

• that the school meets the e-safety technical requirements of any relevant Local Authority E-Safety Policy and guidance

DRAFT

• that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed

• that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant 7

• that the use of electronic media is regularly monitored in order that any misuse / attempted misuse can be reported.

• that only authorised software should be installed on the school ICT systems.

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/*online safety policy and practices
- they have read, understood and signed the staff acceptable use policy.
- they report any suspected misuse or problem to the *Headteacher/DSL/Online Safety Lead* for investigation/action/sanction
- all digital communications with students/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 understand and follow the Online Safety Policy and acceptable use policies
- students 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 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 (DSL)

should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

• sharing of personal data

• access to illegal / inappropriate materials

• inappropriate on-line contact with adults / strangers • potential or actual incidents of grooming

• cyber-bullying

DRAFT

Online Safety Lead

The school has a named member of staff with the day to day responsibility for online safety. Currently this is the Designated Safeguarding .

- leads the Online Safety Group
- 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
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- meets regularly with Online Safety *Governor* to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of *Governors*
- reports regularly to Senior Leadership Team

Network Manager

Those with technical responsibilities 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 online safety technical requirements and any *Local Authority* 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 *Headteacher and Senior Leaders; Online Safety Lead and DSL* for investigation/action/sanction
- *that monitoring software/systems are implemented and updated as agreed in school policies*

DRAFT

Students

• are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems.

• 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyberbullying.

• should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Online safety is a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum provides:

- Key online safety messages that are reinforced to students as part of a planned programme of assemblies and tutorial activities
- Students are 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.

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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore support parents in understanding these issues. Parents and carers will be encouraged to support the school 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' section of the website, Edulink and online student records
- their children's personal devices in the school.

Parents/ carers are responsible for:

• endorsing (by signature) the Student Acceptable Use Policy

• monitoring (as far as possible) their children's compliance with the student Acceptable Use Policy

DRAFT

Community Users

Community Users who access school ICT systems / website /VLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

Policy Statements

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. E-Safety education will be provided in the following ways:

• A planned e-safety programme is provided as part of ICT / PHSE / other lessons and is regularly revisited – this will cover both the use of ICT and new technologies in school and outside school

• Key e-safety messages are reinforced as part of a planned programme of assemblies and tutorial / 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

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report). The school will therefore seek to provide information and awareness to parents and carers.

Education & Training – Staff

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

• A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.

DRAFT

• All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies

Technical – infrastructure / equipment, filtering and monitoring

The school is 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 also ensures that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

• School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the relevant policies.

• There will be regular reviews and audits of the safety and security of school ICT systems

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

• All users will have clearly defined access rights to school ICT systems.

• All users will be provided with a username and password

• The "administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in the school safe

• Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

• The school maintains and supports the managed filtering service.

• Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and if the request is agreed, this action will be recorded.

• The activity of users on the school ICT systems is regularly monitored and recorded. Users are made aware of this in the Acceptable Use Policy. Remote management tools are used by staff to control workstations and view user's activity

• An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager who will then pass onto Senior Management

• Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

• An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.

DRAFT

• An agreed policy is in place that forbids any unauthorised users from installing programmes on school workstations / portable devices.

• An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable device

. • The school infrastructure and individual workstations are protected by up to date virus software.

- The Network Manager 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

Curriculum

Staff should reinforce e-safety messages in the use of ICT across the curriculum.

• in lessons where internet use is pre-planned, students are 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 are allowed to freely search the internet, e.g. using search engines, 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, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant 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.

• Students are taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

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

.

- Students are 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.
- *Students are helped to understand the need for the student acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school/academy.*
- *Staff must act as good role models in their use of digital technologies, the internet and mobile devices*

DRAFT

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilizing 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. The mobile technologies usage should be consistent with relevant school polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety education programme.

The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes*	*Yes**Error! Bookmark not defined.*	*Yes**Error! Bookmark not defined.*
Full network access	*Yes*	*Yes*	*Yes*			
Internet only				/	/	/
No network access						

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils' instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

• When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and 15 distribution of images. In

DRAFT

particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.

• Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment unless direct permission has been obtained from the Designated Safeguarding Lead or Deputy Safeguarding Lead in accordance with the acceptable use policy.

• Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

• Students must not take, use, share, publish or distribute images of others without their permission

• Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.

• Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

• Written permission from parents or carers will be obtained before photographs of students are published on the school website (

• Student's work can only be published with the permission of the student and parents or carers in Years 9-11

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

The school will ensure that:

- it has a Data Protection Policy.
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it

DRAFT

- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- it will hold only 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. The school should develop and implement a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- it provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- If a maintained school/academy, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.

DRAFT

- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- data must be encrypted and password protected.
- device must be password protected. (be sure to select devices that can be protected in this way)
- device must be protected by up to date virus and malware checking software
- data must be securely deleted from the device, in line with school/academy policy (below) once it has been transferred or its use is complete.

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
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- will not transfer any school personal data to personal devices except as in line with school policy
- access personal data sources and records 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

DRAFT

Social Media - Protecting Professional Identity

.

Wadham School has a duty of care to provide a safe learning environment for students and staff. .

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:

- Ensuring that personal information is not published
- Training is provided including: 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 students, 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* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *The school permits reasonable and appropriate access to private social media sites*

Monitoring of Public Social Media:

- As part of active social media engagement, the social media manager and senior staff will monitor the Internet for public postings about the school
- The school will effectively respond to social media comments made by others according to a defined policy or process

The *school's* use of social media for professional purposes will be checked regularly by the DSL officer and Online Safety Lead to ensure compliance with the school policies.

Communications

DRAFT

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				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓				✓			
Use of mobile phones in lessons		✓				✓		
Use of mobile phones in social time	✓				✓			
Taking photos on mobile phones or other camera devices		✓				✓		
Use of personal email addresses by staff to communicate with student				✓				
Use of school email for personal emails				✓				✓
Use of professional forums and facilities	✓						✓	
Use of instant messaging eg Snapchat		✓						✓
Use of social networking sites		✓					✓	
Use of professional blogs	✓						✓	
Use of text messaging by student to communicate with students		✓			✓			

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.

• Users need to be aware that email communications may be monitored

• Users must immediately report – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

• Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.

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 certain internet usage as follows:

User Actions		Acceptable	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images			✓
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation			✓
	adult material that potentially breaches the Obscene Publications Act in the UK			✓
	criminally racist material in UK			✓
	pornography		✓	
	promotion of discrimination		✓	
	promotion of racial or religious hatred			✓
	threatening behaviour, including promotion of physical violence or mental harm			✓
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute		✓	
Using school systems to run a private business			✓	

Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school		✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions		✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)		✓	
Creating or propagating computer viruses or other harmful files		✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet		✓	
On-line gaming (educational)	✓		
On-line gaming (non educational)		✓	
On-line gambling		✓	
On-line shopping / commerce		✓	
File sharing	✓		
Use of social networking sites	✓		
Use of video broadcasting eg Youtube	✓		

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve potentially illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- criminally abusive behaviour

• radicalisation or terrorist related material

• other criminal conduct, activity or materials

the following protocol will be followed:

• Report to a senior colleague

• Senior colleague will consult with another Senior colleague in order to arrive at a judgment as to the seriousness of the incident

• If appropriate an investigation will begin with a conversation with those involved in the incident

• For students, parents will be informed and a sanction may be put in place

• For staff, any investigation will proceed in accordance with staff disciplinary procedures

• Where there may be evidence of criminal activity, the Headteacher will decide if the police will be involved

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 an appropriate 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 shown:

- Disciplinary action may include warning, suspension or dismissal

DRAFT

Students / Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓		✓			
Unauthorised use of non-educational sites during lessons						✓		✓	✓
Unauthorised use of mobile phone / digital camera / other handheld device						✓		✓	✓
Unauthorised use of social networking / instant messaging / personal email						✓	✓	✓	✓
Unauthorised downloading or uploading of files						✓	✓	✓	✓
Allowing others to access school network by sharing username and passwords			✓	✓					✓

DRAFT

Attempting to access or accessing the school network, using another student's / pupil's account						✓	✓	✓	✓
Attempting to access or accessing the school network, using the account of a member of staff			✓	✓			✓	✓	✓
Corrupting or destroying the data of other users			✓	✓	✓	✓	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓	✓	✓		✓	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions				✓	✓	✓	✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			✓			✓	✓	✓	✓
Using proxy sites or other means to subvert the school's filtering system			✓	✓		✓	✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident			✓			✓	✓	✓	✓
Deliberately accessing or trying to access offensive or pornographic material					✓	✓	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			✓	✓		✓	✓	✓	✓

Staff

Incidents:	Refer to line managerr	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Disciplinary action *
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓		✓		✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓	✓				
Unauthorised downloading or uploading of files	✓	✓				
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓	✓				✓
Careless use of personal data eg holding or transferring data in an insecure manner	✓	✓				
Deliberate actions to breach data protection or network security rules	✓	✓	✓	✓		✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓		✓		✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓		✓		✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	✓	✓		✓	✓	✓

Actions which could compromise the staff member's professional standing	✓	✓				✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓				✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓			✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓				✓
Deliberately accessing or trying to access offensive or pornographic material	✓	✓		✓		✓
Breaching copyright or licensing regulations	✓	✓				✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓				✓

*Disciplinary action may include warning, suspension or dismissal

DRAFT