Academy@Worden

Online Safety Policy 2023

ONLINE SAFETY POLICY

RATIONALE

Academy@Worden faces the challenge of trying to keep pace with technological change. It recognises the many opportunities available from such change: opportunities to further empower young people in their education and learning and opportunities to enhance their creativity and skills in communication. However, the school also acknowledges and seeks to protect its community against the inherent risks of the new technologies, risks which cannot always be immediately identified, given the speed of change. Overall, there is the belief that the educational and social opportunities of the new technologies far outweigh the dangers.

This Policy sets out the school's position regarding the use of social networking sites and other forms of social media. The aim of the document is to ensure that all employees are fully aware of the risks associated with using such sites and their responsibilities with regards to the safeguarding and protection of both children and themselves.

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 use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote Student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. The school has a duty of care to its Students and despite the immense educational potential of ICT, there is an unsavoury side to the internet and other current aspects of technology use on mobile devices, which it would be irresponsible to ignore. 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
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- 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.

VALUES AND PRINCIPLES

- To promote safe and responsible use of the new technologies, both within school and in the wider lives of Students. It is recognised that young people need frequent education and guidance to embed and reinforce Online Safety messages.
- To ensure that an intrinsic part of the teaching is not only information and the building of skills but also, at an appropriate level for Student maturity and understanding, discussion of attitudes and values and the ways that new technologies can impact on the quality of personal relationships.
- To help Students to acquire the skills for making considered, informed decisions and for accepting the responsibility for the consequences of these decisions.
- To help Students to learn how to recognise and avoid exploitation and abuse.
- To help Students access appropriate advice and support when necessary.

CONTEXT

Many of the risks outlined above reflect situations in the off-line world and this Online Safety policy links with other school policies e.g.: Behaviour for Learning, Anti-Bullying, Mobile Phone & Smartwatch, Student Acceptable Behaviour Agreement, Safeguarding & Child Protection Policy and Procedures.

As with all other risks, it is impossible to eliminate all risks completely. We aim 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 and be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

GUIDELINES

- The Online Safety policy is reviewed in detail by the Network Manager, Curriculum Leader for ICT and ICT Link Governor each year. Feedback on the work on Online Safety is sought from staff, Students and parents. For example: through the letters to parents which follow the use of the 'Think U Know' resource; the Year 7 ICT Internet Safety Assembly etc
- E-learning takes place in both formal and informal ways. There are dedicated ICT lessons for all Students but use of new technologies is encouraged and is intrinsic in most, if not all, subject areas. Some use lies clearly within the parameters of the school day but other use may be outside of school, for instance in the use of the internet to access information for homework or the use of Web 2.0 technologies. It is neither realistic nor practical to expect that all use can be under adult supervision, either that of adults in school or parents. Young people generally embrace new technology with enthusiasm, they generally know more about it than many adults around them and thus the aim must be to help them to develop a set of safe and responsible behaviours to support them whenever they are online.
- The school will aim to use curriculum opportunities, both in ICT and other subject areas, to provide digital literacy education, helping to teach young people to become critical and discriminating users of materials they find online and through 'direct contact' services such as e-mail, chat or social networking sites. In ICT lessons they will be taught to be aware of the various technological approaches to minimising risk.
- The continued development of effective Online Safety strategies will involve governors, all staff, Students and parents.
- The school will work within LA and police guidelines for Online Safety and make use of support available.

- A member of the Senior Leadership Team is the designated Online Safety Co-ordinator with the aim of ensuring that policy is current and that any breaches or abuse are reported to the Headteacher and dealt with. The aim is always to be consistent and appropriate in dealing with any breaches of Online Safety, using the police when necessary.
- The SLT lead will work closely with those with more detailed day to day knowledge: Network Manager, ICT Technicians and Curriculum Leader for ICT. This is to ensure that technological solutions to Online Safety support classroom practice.
- Feedback will be given to the Governors' Pastoral Sub Committee. The Network Manager will also aim to regularly review and make sure that all staff receive relevant information about any emerging Online Safety issues.
- The ICT Acceptable Behaviour Policies for staff, Students, parents and visitors to the school are at the centre of good practice.
- Upon appointment all staff sign the Worden ICT Acceptable Behaviour Policy. All staff are expected to maintain an appropriate level of professional conduct in their own ICT use both within and outside school. This includes the use of social networking sites.
- Parents sign and return an agreement that their child will comply with the Academy's ICT Acceptable Behaviour Policy.
- Senior Leadership acknowledge the importance of a staff development programme that deals with both the benefits and the risks of communication technologies. Varied strategies are used in staff training, for example inclusion of this aspect in the process of induction of new staff, presentations at staff meetings and practical training from ICT staff.
- Within the context of whole school policy subject leaders will develop relevant Online Safety guidelines for their departments and record these in their departmental handbooks. These will include: embedding Online Safety in the context of that subject curriculum; setting out the procedures that departmental staff are expected to follow in particular subject locations so that Students can be suitably supervised; clear procedures for the immediate reporting of any issues of concern and review through departmental meetings.
- The rate and range of technological development have also led to increasing concerns regarding Online Safety. The pastoral team are most often the members of staff who link with parents over Online Safety issues that occur out of school time but also have knock on effects within school. They will both individually and collectively ensure that matters are followed up via the established procedures within school to ensure consistency, suitable help to Students / parents and, as far as possible, pre-empt future problems.
- All staff who use ICT in the classroom have a duty to ensure that Students are reminded about appropriate behaviour on a regular basis. The main rules will be displayed in all classrooms with computers. Staff need to remember that although filtering systems are generally effective they are not completely fool proof and thus safe and responsible use of the technologies is expected at all times. Students should be regularly reminded about how to seek help and report incidents.
- There are ICT guidelines for all staff informing them of the expected professional behaviour in relation to use of the internet, school equipment and conduct beyond school. There is also specific LA Guidance on the use of social networking sites. See Appendix 4.
- School personal data is collected, stored and used according to the principles of the Data Protection Act (1998) and the General Data Protection Regulation (GDPR).

- The school reserves the right to check any ICT device in the school, including any belonging to Students (or technically to their parents) if there are grounds to suspect it has been used in any way contrary to this policy.
- When using websites all staff will be mindful of the matter of copyright. Students will be encouraged to look for copyright information on sites visited, so reinforcing their understanding of this important issue.
- In production of class and homework, staff will make students aware that plagiarism is not only cheating but that, where sufficient is copied, an illegal infringement of copyright also constitutes a criminal offence.

AIMS AND OBJECTIVES OF THE POLICY

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 online safety is therefore an essential part of the school's Online Safety provision. Students need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online Safety education will be provided in the following ways:

- All Students sign the Academy's ICT Acceptable Behaviour Policy.
- A planned online safety programme will be provided as part of ICT, PHSE and House and Whole School Assemblies and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. It will also regularly cover Cyberbullying.
- The 'Think U Know' resource will be delivered to all Students by their Tutors in PSHE lessons. This resource (or relevant updated program) will be used with each new Year 7 intake. The lesson(s) are followed up with a letter to parents informing them of the work done and asking that they themselves view the CEOPs website.
- Key Online Safety messages will be reinforced as part of a planned programme of assemblies e.g. during Safer Internet Week, National Anti-Bullying Week.
- Students 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
- Students will be helped to understand the need for the Student ABP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school. This message will be reinforced each time Students access computers in school via screen log in.
- Students will be taught to reference and acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms.
- Staff should act as good role models in their use of ICT, the internet and mobile devices
- Posters and displays will be made around school to reinforce the message of staying safe on the internet.

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 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).

- Considering that Parents have a key role in creating safe ICT learning at home and outside the school environment, Worden will aim to further develop strategies in working with parents in this respect and in increasing parental awareness of the messages taught in school.
- The school will therefore seek to provide information and awareness to parents and carers through: Letters, newsletters, web site, ICT lessons, Parents evenings and synergy
- Making Parents aware through information letters about how to report abuse and the misuse of technology – CEOPS.
- The school will regularly update parents with online safety concerns brought about as a result of incidents in school or brought into school in relation to particular websites or social networking sites.

Education & Training – Staff

All staff will 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. An audit of the online safety training needs of all staff will be carried out regularly by the Network Manager.

• All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Behaviour Policies

• This Online Safety policy and its updates will be presented to and discussed by staff on staff INSET days.

Training – Governors

Governors should take part in Online Safety training awareness sessions, with particular importance for those who are members of any sub-committee involved in ICT, Online Safety, Health and Safety, Anti Bullying and Child Protection. This may be offered in a number of ways:

• Attendance at training provided by the Local Authority / National Governors Association / LGfL or other relevant organisation.

• Participation in school training

• Participation in information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their Online Safety responsibilities:

• School ICT systems will be managed in ways that ensure that the school meets the Online Safety technical requirements outlined in the LGfL Security Policy and Acceptable Behaviour Policy and any relevant Local Authority Online Safety Policy and guidance

• There will be reviews/ audits of the safety and security of school ICT systems conducted by the Network Manager.

• 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. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed by the Deputy Headteacher

• All users will be provided with a username and password by the ICT Network Manager and ICT Assistants who will keep an up to date record of users and their usernames. Staff will be required to change their password every 90 days as part of the school Password Security Policy.
• The "master / administrator" passwords for the school ICT system, used by the Network Manager/Assistant will also be available to the Headteacher or other nominated Senior Leader
• Users will be made responsible for the security of their username and password, 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 provided by EXA.
• Worden has provided enhanced user-level filtering through the use of the Sophos UTM filtering programme and NetSupport DNA software which monitors keystrokes against a database of known keywords and phrases.
• In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
• Any filtering issues should be reported immediately to the IT Manager.
• Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Deputy Headteacher and ICT Forum.
• School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Behaviour Policy.
• Remote management tools are used by staff to control workstations and view user's activity. They will not be used on staff laptops/workstations without prior permission of the staff user.
• Users can report any actual / potential online safety incident to the Network Manager, Curriculum Leader for ICT or Designated Safeguarding Leader in charge of Child Protection. The incident will be reviewed and an appropriate sanction put in place.
• Security measures provided by Sophos UTM are in place to protect the servers, firewalls, routers, wireless systems, workstations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
• For the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system the Network manager and ICT Technicians will supply a user name and password and all "guests" will be allowed to use the guest Wi-Fi.
The downloading of executable files by users is blocked by ICT staff.
• Staff are not permitted any personal use on laptops and other portable devices that may be used out of school that belong to school.
• Staff can contact the Network Manager so that they can be allowed to / be forbidden from installing programmes on school workstations / portable devices. Using NetSupport DNA, software can be packaged up and distributed to allow staff to 'pull' the software from a repository and be installed.
•Agreed guidelines are in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices
• The school infrastructure and individual workstations are protected by up to date anti-virus software.
• Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
Laptop hard drives are encrypted using Sophos Safeguard Disk Encryption.

Curriculum

Online Safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

• in lessons where internet use is pre-planned, it is best practice that 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.

• Where Students are allowed to freely search the internet, e.g. using search engines, staff should be 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 staff) 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 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 should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

•Students should be made aware that the playing of games (unless of an educational nature approved by staff e.g.: MyMaths, BBC Bitesize) on the internet is strictly forbidden and anyone caught doing so will receive an appropriate punishment

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and Students 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 will inform and educate Students 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.

•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, the personal equipment of staff should not be used for such purposes.

•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, prospectus, or elsewhere that include Students will not be used unless written parental consent has been given.

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

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

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and General Data Protection Regulation (GDPR) which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected and encrypted computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

Consequences

Online safety in taken very seriously and any pupil found to be in breach of the online safety policy or the acceptable use of ICT guidelines will receive appropriate sanctions and support as outlined in the Behaviour and peer on peer abuse policy.

In all cases where a crime has been committed, it will be reported to the Police.

Support

The school has a duty of care to all its pupils and as such the school will always offer pastoral support on an individual basis to each pupil. This pastoral support will vary with every situation.

A risk management plan may need to be put in place and Children's social care may need to be contacted.