Academy@Worden

Online Safety Policy

Last updated: 12 November 2015

Contents:

Last updated: 12 November 2015

Statement of intent

At Academy@Worden we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the academy recognises the importance of promoting the use of computer technology throughout the curriculum, we also recognise the need for safe internet access and appropriate use.

Our academy has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The academy is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

This policy will operate in conjunction with other important policies in our academy, including our Anti-bullying Policy, Data Protection Policy, Child Protection and Safeguarding Policy, Allegations Against Staff Policy and digital safeguarding policy.

Last updated: 12 November 2015

1. Legal framework

1.1. This policy has due regard to the following legislation, including, but not limited to:

- The Human Rights Act 1998
- The Data Protection Act 1998
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspection Act 2006
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006

2. Use of the internet

2.1. The academy understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

2.2. Internet use is embedded in the statutory curriculum and is therefore entitled to all pupils, though there are a number of controls required for the academy to implement, which minimise harmful risks.

2.3. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful. These risks include:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

3. Roles and responsibilities

3.1. It is the responsibility of all staff to be alert to possible harm to pupils or staff, due to inappropriate internet access or use both inside and outside of the academy and to deal with incidents of such as a priority.

3.2. The DSL in conjunction with the Network manager and Head of ICT, are responsible for ensuring the day-to-day online safety in our academy, and managing any issues.

3.3. The headteacher is responsible for ensuring that the staff in the above named roles and any other relevant staff receive continuous professional development to allow them to fulfil their role and train other members of staff.

3.4. The DSL, network manager and Head of ICT will provide all relevant training and advice for members of staff on online safety.

3.5. The headteacher will ensure there is a system in place which monitors and supports the online safety officers (outlined above), whose role is to carry out the monitoring of online safety in the school.

3.6. The online safety officers will regularly monitor the provision of online safety in the school.

3.7. The academy will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.

3.8. Cyber bullying incidents will be reported in accordance with the academy's Anti-Bullying Policy, behaviour policy and safeguarding policy.

3.9. The DSL will ensure that all members of staff are aware of the procedure when reporting online safety incidents, and will keep a log of all incidents recorded.

3.10. The SLT will hold yearly meetings with the online safety officers to discuss the effectiveness of the online safety provision, current issues, and to review incident logs. Findings and recommendations will be reported to the governing body in the form of updated policies.

3.11. The governing body will evaluate and review this online safety Policy on a yearly basis.

3.12. The headteacher/SLT will review and amend this policy with the online safety officers, taking into account new legislation and government guidance, and previously reported incidents to improve procedures.

3.13. Teachers are responsible for ensuring that online safety issues are embedded in the curriculum and safe internet access is promoted at all times.

3.14. All staff are responsible for ensuring they are up-to-date with current online safety issues, and this online safety Policy. However the Head of ICT and DSL will ensure that staff have access to yearly training on the subject.

3.15. All staff and pupils will ensure they understand and adhere to the Acceptable Use Policy, which they must sign and return to the headteacher.

3.16. Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices, appropriately.

3.17. The headteacher is responsible for communicating with parents regularly and updating them on current online safety issues and control measures.

4. Online safety control measures

4.1. Educating pupils:

- An online safety programme will be established and taught across the curriculum on a regular basis, ensuring pupils are aware of the safe use of new technology both inside and outside of the academy.
- Pupils will be taught about the importance of online safety and are encouraged to be critically aware of the content they access online.
- Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be presented in all ICT classrooms.
- Pupils are instructed to report any suspicious use of the internet and digital devices.

4.2. Educating staff:

- All staff will undergo online safety training on a yearly basis to ensure they are aware of current online safety issues and any changes to the provision of online safety.
- All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.

4.3. Internet access:

- Internet access will be authorised once parents and pupils have returned the signed consent form as part of the Acceptable Use Policy.
- A record will be kept by the school of all pupils who have been granted internet access.
- All users in key stage 3 and above will be provided with usernames and passwords, and are advised to keep this confidential to avoid any other pupils using their login details.
- Pupils' passwords will be changed on a regular basis, and their activity is continuously monitored by the network manager and the Impero monitoring software.
- Management systems (Impero) will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.
- Effective filtering systems will be established to eradicate any potential risks to pupils through access to particular websites.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by a senior member of staff.
- All school systems will be protected by up-to-date virus software.
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers and supply teachers etc.

4.4. Email:

- Staff will be given approved email accounts and are only able to use these accounts.
- Use of personal email to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any other pupils, staff or third parties via email.
- Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

4.5. Social networking:

- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by a senior member of staff (SLT).
- Pupils are regularly educated on the implications of posting personal data online, outside of the academy.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the academy as a whole.
- Staff are not permitted to communicate with pupils over social networking sites unless this is done via the official school networking account with prior consent from the headteacher.

4.6. Published content on the academy's website and images:

- The business manager will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- All contact details on the academy website will be the phone, email and address of the academy. No personal details of staff or pupils will be published.
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Pupils are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take images, though they must do so in accordance with academy policies in terms of the sharing and distribution of such. Staff will not take images using their personal equipment.

4.7. Mobile devices:

- The headteacher or a member of the SLT may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.
- Mobile devices are not permitted to be used in the classroom by pupils.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- The academy will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

5. Cyber bullying

5.1. For the purpose of this policy, "cyber bullying" is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images, online.

5.2. The academy recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

5.3. The academy will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.

5.4. The academy will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.

5.5. The academy has zero tolerance for cyber bullying and other bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-bullying Policy.

5.6. The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a pupil.

6. Reporting misuse

6.1. Misuse by pupils:

- Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the headteacher in verbal format followed by a written account.
- Any pupil who does not adhere to the rules outlined in our Acceptable Use Policy and is found to be wilfully misusing the internet, will have a letter sent to their parents/carers explaining the reason for suspending their internet use.
- Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the headteacher.
- Complaints of a child protection nature shall be dealt with in accordance with our Child Protection Policy and referred immediately to the DSL.

6.2. Misuse by staff:

- Any misuse of the internet by a member of staff should be immediately reported to the headteacher, using a written format that may well be followed up verbally.
- The headteacher will deal with such incidents in accordance with the Allegations Against Staff Policy, and may decide to take disciplinary action against the member of staff.
- The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.