

Academy@Worden



Digital Safeguarding Policy

Contents:

Statement of intent

- 1) Introduction
- 2) Aims
- 3) Definition
- 4) Online safety measures
- 5) School policies
- 6) Monitoring

Statement of intent

This policy is intended to ensure pupils at Academy@Worden are protected while using digital technologies at the school.

The academy is committed to including digital technologies, in particular internet use, in our curriculum. In doing so, we recognise the inherent risks posed by this useful learning tool. Full compliance with this policy will mitigate these risks and help to ensure pupils are safe online.

1. Introduction

- 1.1. While digital technology and the internet provide an exciting opportunity for pupils to learn and interact with various subjects, they also pose a risk, with the potential for exposure to inappropriate content and inappropriate contact from other children and adults. Digital technology also provides an opportunity for pupils to engage in unacceptable behaviour, both online and offline.
- 1.2. In order to keep pupils safe online, and for them to learn how to keep themselves safe online, all pupils and teachers should be aware of relevant skills and strategies needed to ensure online safety. This ranges from knowing to only use the internet with adult supervision for younger pupils, to strategies for identifying appropriate links for older children.
- 1.3. Mitigating the risk to pupils created by digital technology and the internet will be ensured through specific safety lessons and will also be embedded within the general curriculum.
- 1.4. Online safety will depend on policies being properly implemented at all levels of the school community: from published policies, to a secure school network design, the effective management of school broadband and filtering systems, parental awareness of the dangers of online use and effective teaching about digital-technology use.
- 1.5. This policy is to work in conjunction with our Safeguarding Policy, online safety policy, electronic device policy and acceptable use of ICT policy.

2. Aims

- 2.1. At Academy@Worden, we are committed to using the internet and other digital technologies to:
 - Make learning more exciting and interactive.
 - Make lessons more varied.
 - Enable pupils to gain access to a wide variety of knowledge in a safe way.
 - Raise educational standards.
 - Prepare our pupils for using the internet safely outside of school and throughout their education.

3. Definition

- 3.1. Digital safety encompasses a number of technologies such as computers, tablet computers, collaboration tools, internet technologies, mobile devices and any other electronic device that is used around the school that can access the internet).

4. Online safety measures

- 4.1. The academy's internet system, and access to it, is specifically designed for staff and pupil use and, as such, includes filtering appropriate for school age children and as such this is provided by the LA.
- 4.2. Pupils will have clear objectives about why they are using the internet whenever the internet is incorporated into lessons.
- 4.3. Lessons using the internet will be carefully planned and the 'access levels' classes and pupils are afforded will be fully considered, taking into account pupil age and curriculum requirements.
- 4.4. Children using the internet will do so in classrooms (or other appropriate shared areas of the school) during lesson time only and with teacher supervision.
- 4.5. Pupils will be taught what internet use is acceptable and unacceptable, and teachers should be vigilant during internet based lessons.
- 4.6. Particular vigilance is necessary if and when pupils are undertaking internet searching. Teachers should use their professional judgement regarding whether this internet function is appropriate for the relevant class.
- 4.7. If the Google images website is used in class, this should be done using the 'safe search' function. Teachers can make judgement calls on whether to allow the use of Google images at all, due to the range of content and possibility for accessing inappropriate material.
- 4.8. Records will be maintained detailing all staff and pupils who have internet access.
- 4.9. Impero monitoring software is active on all computers within school and provides an extra level of security and monitoring at a background level.

5. School policies

- 5.1. Information system security:
 - 5.1.1. Academy@Worden uses Lancashire County Council Broadband services with the appropriate firewall and all appropriate filters provided by LCC as well as Impero for extra in school filtering and monitoring.
 - 5.1.2. The security of the information systems and ICT system capacity will be reviewed regularly.
 - 5.1.3. The virus protection will be regularly updated. There should be procedures in place for virus protection to be updated on any laptops used by staff members or students.
- 5.2. Email and digital communications:

- 5.2.1. Only approved school e-mail accounts may be used at school/via the school network. Additionally, pupils must not receive or access personal e-mail accounts.
- 5.2.2. Pupils should notify a teacher immediately if they receive an offensive e-mail.
- 5.2.3. Pupils should be taught about the dangers involved in e-mail communications. They should be taught:
 - Not to reveal personal details about themselves or others in e-mail or digital communication. This will generally include full names, addresses, mobile or landline phone numbers, school name, instant messenger (IM) address, e-mail address, names of friends, specific interests and clubs etc.
 - Never to arrange to meet someone they have 'met' via e-mail/online without appropriate safeguarding measures (e.g. the presence of a parent or responsible adult).
 - That online communications are 'real' and as such require the same respect for others as face-to-face interactions.
- 5.2.4. Parents and pupils alike should both be informed of the risks inherent in using social media. Social media websites will not be accessible through the school's network and should not be accessed on school devices through other networks.
- 5.2.5. The school's network manager will maintain a list of 'inappropriate' and 'banned' terms. The use of these in e-mails will be detected and logged.
- 5.2.6. Whenever staff or pupils send e-mails to organisations or persons outside of the school, these should be authorised in the same way official school correspondence would be.
- 5.3. The school website:
 - 5.3.1. The school business manager has overall responsibility for the content of the school website. This includes ensuring all content is appropriate and accurate. There are procedures in place for authorising the uploading of any content onto the school's website.
 - 5.3.2. No personal information or contact details will be published on the school's website. This extends to the use of pupil's full names. The school address, e-mail and main telephone number should be the only contact information available to website visitors.
 - 5.3.3. The uploading of any images or photographs of pupils onto the school website requires parental permission in writing that is obtained when a pupil joins the school. Any images should be carefully chosen with safeguarding in mind and it is advisable that pupils are not easily identifiable in images.

5.4. Managing filtering:

- 5.4.1. The ICT department will work to ensure filtering systems are appropriate, efficient and as effective as possible. This will entail regular checks and ongoing monitoring.
- 5.4.2. If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the Network manager. There are processes in place to deal with such reports.

5.5. Protecting personal data:

- 5.5.1. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

5.6. Complaints:

- 5.6.1. Complaints regarding pupil misuse of the school's internet/digital devices will be dealt with by the network manager and an appropriate, senior member of staff (Deputy or Assistant Headteacher). Sanctions for misuse may include:

- Revocation of internet use privileges
- Communication with the pupil's parents/carers
- Detention or other usual discipline methods
- Exclusion from school

- 5.6.2. Staff misuse of the internet or digital technology should be referred to the headteacher.

- 5.6.3. Any issues or complaints of a child protection nature should be dealt with according to the school's Child Protection and Safeguarding Policy procedure.

- 5.6.4. Information on the complaints procedure should be published on the school's website and parents should be informed about this.

5.7. Digital technology/internet use outside of school:

- 5.7.1. Parents should be informed of the inherent risks of internet use.

- 5.7.2. The school will be aware of, and responsive to, any issues pupils experience via their use of the internet or digital technology outside of school. The school provides useful information for parents on the website as well as holding an annual Internet safety evening.

6. Monitoring

- 6.1. The law related to internet use is changing rapidly and staff and pupils need to be aware of this. Relevant laws include:

- The Computer Misuse Act 1990
- The Public Order Act 1986

- The Communications Act 2003
- The Sexual Offences Act 2003
- The Malicious Communications Act 1988
- The Copyright, Design and Patents Act 1988
- The Protection of Children Act 1978
- The Obscene Publications Act 1959 and 1964
- The Protection from Harassment Act 1997

6.2. This policy should be monitored and updated to account for changes in the legal landscape, such as amendments to the outlined laws. The school business manager, network manager and deputy headteacher are responsible for updating this policy and ensuring the school remains in compliance with its legal obligations.