Coupals Primary Academy

Digital Safeguarding Policy

Last updated: 25 August 2019

Contents:

Statement of intent

This policy is intended to ensure pupils at Coupals Primary Academy 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.

Signed by:

________________ Headteacher Date: ________________

________________ Chair of governors Date: ________________

1. Introduction

1.1.

2. Aims

2.1. 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.

2.2. 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 internet 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.

2.3. 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.

2.4. 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.

2.5. This policy is to work in conjunction with our Safeguarding Policy.

2.6. At Coupals Primary Academy, 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

Digital safety encompasses a number of technologies such as computers, tablet computers, collaboration tools, internet technologies, mobile devices and online learning platforms

4. E-safety measures

4.1. The Coupals Primary Academy internet system, and access to it, is specifically designed for staff and pupil use and, as such, includes filtering appropriate for primary age children.

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 about online safety as part of the curriculum.

4.6. In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private

- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

4.7. Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly

- Recognise acceptable and unacceptable behaviour

- Identify a range of ways to report concerns about content and contact

4.8. Particular vigilance is necessary if and when pupils are undertaking internet searching (to monitor content to ensure it is not inappropriate or extremist – as per the schools commitment to the Prevent Strategy to minimise radicalisation). Teachers should use their professional judgement regarding whether this internet function is appropriate for the relevant class.

4.9. 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.

4.10. To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

4.11. Inappropriate usage and all incidents causing concern will be recorded on CPOMS and brought to the attention of the DSL.

5. School Policies

5.1. Information system security:

- Coupals Primary Academy uses E2BN with the appropriate firewall and all appropriate filters.
- The security of the information systems and ICT system capacity will be reviewed regularly.
- 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:

- 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.
- 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 and images or information which identify the pupils' school 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.

- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

5.2. 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.

5.3. Whenever staff send e-mails to organisations or persons outside of the school, these should be authorised in the same way official school correspondence would be.

5.4. The school website:

- The Headteacher and governing body have 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.

- 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.

- The uploading of any images or photographs of pupils onto the school website requires parental permission in writing. Any images should be carefully chosen with safeguarding in mind and it is advisable that pupils are not easily identifiable in images. Pupil's names should never be used in conjunction with their photograph on the website.

5.5. Managing filtering:

- The IT team will work to ensure filtering systems are appropriate, efficient and as effective as possible. This will entail regular checks and ongoing monitoring. This includes the filtering of extremist materials in line with the schools commitment to the government's Anti-Radicalisation Prevent strategy.

- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the IT team. There are processes in place to deal with such reports.

5.6. Protecting personal data:

Personal data will be recorded, processed, transferred and made available according to the GDPR 2018, see GDPR policy.

5.7. Complaints:

Complaints regarding pupil misuse of the school's internet/digital devices will be dealt with by the Headteacher/Deputy Headteacher. Sanctions for misuse may include:

- Revocation of internet use privileges

- Communication with the pupil's parents/carers

• Accurate record on CPOMS

5.8. Staff misuse of the internet or digital technology should be referred to the Headteacher.

5.9. Any issues or complaints of a child protection nature should be dealt with according to the school's Safeguarding Policy procedures and recording on CPOMS.

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

5.11. Digital technology/internet use outside of school:

- Parents and children should be informed of the inherent risks of internet use (including the risk of radicalisation through extremist materials).
- Pupils will be taught about the age of criminal responsibility and that inappropriate use of the internet and electronic devices could lead to criminal charges being brought against pupils.
- 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.
- Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 1.
- Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.
- If staff have any concerns over the security of their device, they must seek advice from the ICT manager.
- Work devices must be used solely for work activities.

6. Monitoring

6.1. The DSL logs behaviour and safeguarding issues related to online safety.

6.2. 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

6.3. This policy should be monitored and updated to account for changes in the legal landscape, such as amendments to the outlined laws. The Headteacher is responsible for updating this policy and ensuring the school remains in compliance with its legal obligations.

6.4. This online safety policy is linked to our:

• Child protection and safeguarding policy

• Behaviour policy

• Staff disciplinary procedures

• Data protection policy and privacy notices (is it still called this or is it GDPR?)

• Complaints procedure

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor: ______________________________

When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature

• Use them in any way which could harm the school's reputation

• Access social networking sites or chat rooms that is not for educational purposes

• Use any improper language when communicating online, including in emails or other messaging services

• Install any unauthorised software

• Share my password with others or log in to the school's network using someone else's details

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school may monitor the websites I visit.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's GDPR policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor): ____________________________

Date: ____________________________