Rowde C of E Academy

Digital Safeguarding Policy

Date agreed: September 2020
Reviewed: September 2021
Next Review Date: July 2021

This policy is intended to ensure pupils at Rowde School are protected while using digital technologies at the school.

Rowde School 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.

Introduction

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.

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.

Mitigating the risk to pupils created by digital technology and the internet will be ensured through specific online safety lessons within the computing and PSHE curriculum.

E-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.

This policy is to work in conjunction with our Safeguarding Policy, Cyber Bullying Policy and Social Media Policy.

Aims

At Rowde School, we are committed to using the internet and other digital technologies to:

- Make learning exciting and interactive.
- 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.

Definition

Digital safety encompasses a number of technologies such as computers, tablet computers, collaboration tools, internet technologies, mobile devices and software.

E-safety measures

The Rowde School internet system, and access to it, is specifically designed for staff and pupil use and, as such, includes filtering appropriate for primary age children. Pupils have individual logins for each machine.

Staff have individual logins for each machine. Teachers have been shown how to lock their computer when they leave a machine unattended. Desktop computers self-lock after 30 minutes of inactivity.

All staff iPads and hardware are password protected.

Staff who take their laptops home should have encryption installed. Staff

should only store data on encrypted memory sticks.

Staff should regularly delete files which contain pupil's names, images from both their own Drive and any documents saved on Staffshare.

Governors have access to a secure Sharepoint to access governor information.

Pupils will have clear objectives about why they are using the internet whenever the internet is incorporated into lessons.

Lessons using the internet will be carefully planned, taking into account pupil age and curriculum requirements.

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.

Key stage 1 pupils should only use the internet with teacher observation or direct teacher supervision.

Pupils will be taught what internet use is acceptable and unacceptable, and teachers should be vigilant during internet based lessons.

Pupils are taught what to do if they access inappropriate content either in school or at home

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.

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.

School policies

Information system security:

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 pupils.

All new programmes installed on the server should be signed off by AET and SLT.

Email, 'Seesaw' 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 on school devices.

Email should be used for appropriate professional use within the school. Emails should not contain inappropriate language or content and should reflect the professional standards of the school, similar to that of a letter sent from the school.

Communication via SeeSaw should always reflect the highest professional standards. When commenting on Seesaw work, staff should leave feedback directly linked to learning and avoid engaging in conversations with parents or pupils via Seesaw.

Staff should always be wary of opening emails from unknown sources through their school email.

Pupils should be taught about the dangers involved in e-mail communications. They should be taught as part of the Digital Literacy strand of the Computing Curriculum:

- 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.

- Pupils who do not have permission for photos to be recorded on Seesaw should not be included in any group posts or blogs.

- Parents should give permission for their child to be included in Seesaw posts.

- Parents and pupils should never share home learning codes on social media or any other public platform.

- Pupils should use Seesaw at home to complete home learning activities as directed by the teacher.

- 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 (as referenced in the school social media policy).

- Whenever staff send e-mails to organisations or persons outside of the school, these should be considered in terms of their formality and confidentiality and in some cases emails / documents should be encrypted or password protected. Children should not be named in emails (initials and d.o.b preferred).

The school website

The Headteacher and Business Manager have overall responsibility for the content of the school website. The management of the website is shared between the admin team, Head and Computing lead in the school. This includes ensuring all content is appropriate and accurate. There are procedures in place for authorising the upload 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. Pupil's names should never be used in conjunction with their photograph on the website.

Managing filtering

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.

If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the Headteacher. There are processes in place to deal with such reports. Protecting personal data:

Personal data will be stored in accordance to the school's GDPR policy and as such the General Data Protection Policy (2018)

Complaints

Complaints regarding pupil misuse of the school's internet/digital devices will be dealt with by the Head or a senior member of staff.

Sanctions for misuse may include:

- Revocation of internet use privileges
- Communication with the pupil's parents/carers

School's Behaviour and Attitudes policy

Staff misuse of the internet or digital technology should be referred to the Headteacher and potentially may lead to disciplinary action.

Pupil misuse of technology will be dealt with through the school behaviour policy

The school will actively involve itself in dealing with misappropriate

Any issues or complaints of a child protection nature should be reported to the Designated Safeguard Leader and dealt with according to the school's Child Protection and Safeguarding Policy / procedure.

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

Digital technology/internet use outside of school:

Parents should be supported by the school to better understand the inherent risks of different applications and internet use.

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's Cyber Bullying Policy may also be relevant in such instances.

Monitoring

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
The General Data Protection Policy 2018

This list is not exhaustive and will be subject to updates from time to time. The school will comply with latest version of the above legislation.

YouTube

YouTube can be an effective teaching resource in schools and provides exciting and engaging educational stimuli within lessons. However increasingly, content including video and written text on the YouTube website can contain content inappropriate to be viewed by children of a primary school age. As responsible adults within the school it is our duty to safeguard children and ensure any materials used within the class are suitable and relevant to the learning taking place.

It is the adult's responsibility to check all content shown to children within the school **prior** to using it in class.

There should always be a justifiable educational reason for accessing YouTube content.

Teachers should be in control of any device including laptop or interactive whiteboard whenever YouTube is displayed in the class.

Children should not be accessing any machine with a staff login unsupervised

Teachers should avoid searching for a video using the YouTube search. This can display a range of videos which could be inappropriate.

To access videos safely, create a Hyperlink to the videos through a Microsoft Word document for example the teacher's weekly planning or embed video into Microsoft PowerPoint prior to using in class. This will avoid any 'pop up' material being displayed.

Any failure to apply due care whilst using YouTube could result in disciplinary measures. Please sign the section below and pass to the Head teacher.

Other Content Streaming Services

Staff should be mindful about accessing or displaying content from any online digital streaming platform such as BBC iPlayer or Netflix. Staff should vet any content to ensure it is suitable for the age viewed (Any content rated beyond 'U' requires parental consent). They should also be mindful of adverts which may be displayed before any content is shown.
It is the responsibility of the staff member **logged onto the device** for which content is shown.

Linked Policies:
Rowde Child Protection Policy
Behaviour Policy
Social Media Policy
Cyber-bullying policy
GDPR policy

Rowde School - Digital Safeguarding Policy

I have read, fully understand and will comply with the above policy regarding the use of 'YouTube' in school.

Name:_____ Signed: _____

Date: _____