# Scargill Church of England Primary School

# E-Safety Policy

Approved: March 2021

Review date: March 2023

## 1.0

## Context

“The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom.”

DfES, eStrategy 2005.

At Scargill C of E Primary School we recognise that learning is a lifelong process and that e-learning is an integral part of it. Ensuring that we provide pupils with the skills to make the most of information and communication technologies is an essential part of our curriculum.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the ‘virtual’ or digital world as would be applied to the school’s physical buildings. This Policy is drawn up to protect all parties – the students, the staff and the school. It aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

## 2.0

## Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Technologies which might be used in school, and quite often outside school, include;

- Email
- Blogs
- Instant messaging
- Podcasting
- Social networking sites
- Chat rooms
- Gaming sites
- Music download sites
- Mobile phones and Smart phones including use of camera and video functionality
- Tablets
- Smartwatches

**3.0**

## Roles and Responsibilities

We aim to embed safe practices into the culture of our school, promoting and supporting safe behaviours in the classroom. Therefore the implementation of this policy is the responsibility of all the staff that work with the children in the school. It is the responsibility of the Head teacher and the ICT coordinator to ensure that this takes place.

**4.0**

## School Website

Our school website scargill.derbyshire.sch.uk

- Is the official site with main contact details, prospectus information and other information which may be of use to parents, pupils and the general public
- This website is the editorial responsibility of the Head teacher, senior leadership team and the computing leader who ensure that the content is accurate
- Photographs or personal details, which could identify individual students, will not be published on the website without permission from parents

**5.0**

## Managing the Network and Equipment

This school:

- Scans all mobile equipment with anti-virus/spyware before it is connected to the network
- Asks staff to ensure that equipment which goes home has the anti-virus and spyware software maintained up-to-date
- Has set up the network with a shared work area for pupils and one for staff
- Provides pupils with year group log-ins/passwords for the network and staff with individual log-ins/ passwords
- Makes it clear to staff and pupils that no-one should log on as another user
- Provides pupils and staff with remote access to content and resources through the approved Learning Platform which is accessed using individual usernames and passwords
- Ensures that all pupil level data or personal data sent over the internet is encrypted or sent within the approved secure system in our LA or through USO secure file exchange
- Has a wireless network which has been secured to industry standard Enterprise security level / appropriate standards suitable for educational use

## 6.0

## Managing the Internet Safely

This school

- Uses a filtering system which blocks sites which fall into categories such as pornography, race hatred, gaming, sites of an illegal nature etc
- Uses Sophos anti-virus software so staff and pupils cannot download executable files
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes
- Blocks all chat rooms and social networking sites except those which are part of an educational network or approved learning platform
- Provides staff with an email account for their professional use
- Is vigilant in its supervision of pupils
- Is vigilant when conducting a 'raw' image search with pupils e.g. Google
- Asks staff and pupils to sign a 'use of agreement' form

## 7.0

## Infringements by Students

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons
- Use of unauthorised instant messaging/social networking sites
- Sending an email or message that is regarded as offensive, harassment or of a bullying nature
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet

## 8.0

## Infringements by Staff

- Excessive use of internet for personal activities not related to professional development eg online shopping, personal email, instant messaging etc
- Serious misuse of, or deliberate damage to, any school/Council computer hardware or software
- Any deliberate attempt to breach data protection or computer security rules
- Deliberately accessing, downloading and disseminating material deemed offensive, obscene, defamatory, racist, homophobic or violent

**9.0**

## Complaints and Concerns regarding E-Safety

Staff and students are given information about uses that are considered infringements, and possible sanctions. Sanctions available include:

- Discussion with Headteacher
- Informing parents or carers
- Removal of Internet or computer access for a period
- Referral to MAT/Police
- Other disciplinary action according to school's codes

The head of school or computing leader acts as first point of contact for any complaint.

Complaints of cyberbullying should be dealt with in accordance with our Anti-Bullying Policy.

Complaints related to child protection should be dealt with in accordance with school/MAT child protection procedures.

If a member of staff commits an exceptionally serious act of gross misconduct then school is likely to involve external support agencies as part of these investigations eg an ICT technical support service to investigate equipment and data evidence, and the MAT Human Resources team.

This policy has been formally approved and adopted by the Governors at a formally convened meeting.

Policy approved: ________________________________________

Date: ________________________________________

Date of Policy review: ________________________________________

**End of statement**

**Scargill C of E Primary School Staff e-safety rules / Code of conduct**

ICT and the related technologies such as email, the internet and mobile phones are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs Hallsworth, Head of School, or Mr Attenborough, ICT/E-safety coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes
- I will comply with the ICT system security and not disclose any passwords provided to me by the school
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will only use the approved, secure email system(s) for any school business
- I will not browse, download or upload material that could be considered offensive or illegal
- I will not send to pupils or colleagues material that could be considered offensive or illegal
- Images of pupils will only be taken and used for professional purposes and will not be distributed outside the school network without the permission of the parent/ carer
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies
- I will report any misuse or inadvertent exposure to inappropriate conduct
- I understand that any infringement of these rules maybe treated as misconduct or gross misconduct

## User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ……..………………….……………………………..     Date ……………………

Full Name ……………………………………………………………………….     (printed)

Job title……………………………………………………………………………….

## Scargill C of E Primary School Pupil e-Safety Rules

- At school I will only use ICT, such as the internet, email, digital video etc with permission from a teacher.
- I will only access the school network using my own user name and password.
- I will be responsible for my behaviour when using the Internet.
- I will only send messages that are polite and friendly.
- I will not deliberately look at websites that could be offensive to anyone, or illegal.
- If I accidentally come across anything that could be offensive or illegal I will immediately tell my teacher.
- I will not send anything that could be threatening, offensive or illegal to pupils, teachers or others.
- When I use the internet I will not give out any personal information such as my name, phone number or address.
- I will not arrange to meet anyone unless this is part of a school project and is approved by my teacher.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

## E-SAFETY INCIDENT REPORTING FORM

| | |
|---|---|
| Date of incident: | |
| Member of staff reporting incident: | |
| Url, (web address) of incident: | |
| Copy of screens/evidence saved to: | |
| Location of incident (room): | |
| Computer number if known: | |
| Details: | |
| Passed to: | |
| Action taken | |