STOKES WOOD
PRIMARY SCHOOL

ICT Acceptable Use Policy

This policy should be read in conjunction with the following policies:

- Social Media Policy
- Remote Learning Policy

Approved by:	**Date:**
Last reviewed on:	
Next review due by:	

Contents

---

1. School Vision

Stokes Wood Primary School is an ambitious place. We aim to help every child become a global ambassador, ready to explore and understand the world around them. We encourage our children to be curious, ask questions and seek answers as they learn. Our children are confident in sharing their ideas and opinions. They know how to listen and communicate with kindness and respect. We believe in a community where there are no outsiders– everyone belongs and every voice is heard. Above all, we nurture their well-being, ensuring they grow into healthy, balanced individuals committed to lifelong learning and positive change. Together, we create a caring and supportive environment where everyone can grow and succeed, ready to make a positive difference in Leicester and beyond!

Purpose

As a professional organisation with responsibility for children's safeguarding it is important that colleagues take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. Everybody has responsibility to use the organisation's computer systems in a professional, lawful, and ethical manner. To ensure that colleagues are fully aware of their professional responsibilities when using Information Communication Technology and the organisations systems, they are asked to read and sign this ICT Acceptable Use Policy (AUP). This is not an exhaustive list and all colleagues are reminded that ICT use should be consistent with the organisations ethos, GDPR regulations, other appropriate policies, relevant national and local guidance and expectations, and the Law.

1. Scope

The policy applies to:

- All employees.
- Information assets, whatever format, device or medium they are held in.
- All Stokes Wood owned information, in whatever format, wherever it is held (e.g. by a third party) for which Hazel Bramley, Business manager, is the data controller.

2. Employee Responsibilities

i. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites.

ii. Stokes Wood Primary School information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to

computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

iii. I understand that any hardware and software provided by my workplace can only be used by colleagues employed by the Trust. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

iv. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 6 or more characters and is changed regularly.

v. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from your line manager or the IT Department.

vi. I will ensure that any personal data of pupils, colleagues or parents/carers is kept in accordance with the General Data Protection Regulation (GDPR). This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any data which is being removed from the school site's (such email) will be encrypted by a method approved by the IT Department. Any images or videos of pupils will only be used in line with organisational policy and will always take into account parental consent.

vii. I will not keep professional documents which contain organisation-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones). If I choose to access the organisations email system on my mobile device (tablet or mobile phone), the device must be pin or password protected. I will protect the devices in my care from unapproved access or theft.

viii. Personal data kept on work devices must be kept to a minimum (examples that do not meet this include; Filling the hard drive with music files or photos).

ix. I will respect copyright and intellectual property rights.

Updated for GDPR – April 2018

x. I have read and understood the Social Media policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

xi. I have carried out Data Protection and GDPR training.

xii. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead (DSL) and line manager as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Designated Safeguarding Lead and your line manager.

xiii. I will not attempt to bypass any filtering and/or security systems put in place by the organisation. If I suspect a computer or system has been damaged or affected by a virus or other malware, to the ICT Department as soon as possible.

xiv. I will report any actual or potential data breaches to the Local Data Protection Representatives with 24 hours of the incident using the agreed Information Security Incident Form.

xv. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via approved communication channels e.g. via a provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking.

xvi. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the organisations AUP and the Law.

xvii. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the organisation I work for into disrepute.

xviii. I will promote online safety and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

xix. I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance. This includes the use of monitoring software on colleague's laptops.

xxi. I understand this forms part of the terms and conditions set out in my contract of employment.