GREAT OAKS SMALL SCHOOL

SAFEGUARDING COMMUNITIES EMBRACING DIFFERENCE UNLOCKING POTENTIAL

(SAFEGUARDING & DATA PROTECTION)

ACCEPTABLE USE POLICY FOR STAFF 2.1

HEAD TEACHER: JULIE KELLY

CHAIR OF TRUSTEES: CLIVE BEST

Date Agreed: April 2019

Date of Next Review: April 2020

At Great Oaks Small School we want to ensure that all members of our community are safe and responsible users of technology.

This policy consists of:

- Part 1: Acceptable Use Policy for Staff
- Part 2: Wi-Fi Acceptable Use Policy

Part 1: Acceptable Use Policy for Staff

As a professional organisation with responsibility for safeguarding, it is important that staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using technology, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list; all members of staff are reminded that IT use should be consistent with the school ethos, school policies, national/local guidance and expectations, and the Law.

1. I understand that Information Systems and IT 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.
2. School owned 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.
3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. 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. I will protect the devices in my care from unapproved access or theft.

4. I will respect system security and will not disclose any password or security information. I will use a 'strong' password to access school systems. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system. Your password MUST contain at least one capital letter. It is a school requirement that network login and SIMS passwords are changed every 30 days and email passwords are changed every 60 days. All removable devices (memory sticks/portable hard drives etc) must be virus scanned. Our system does this automatically but if you are in any doubt please see the IT Manager

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

6. I will ensure that any personal data of students, staff or parents/carers is kept in accordance with the Data Protection legislation (including 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 or accessed remotely.

    - Any data being removed from the school site (such as via email or on memory sticks or CDs) will be suitably protected. This may include data being encrypted by a method approved by the school. No school data is to be stored on a home computer, or un-encrypted storage device.

    - Any images or videos of students will only be used as stated in the school Image Use Policy and will always reflect parental consent.

7. I will not keep documents which contain school-related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones.

8. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

9. I will respect copyright and intellectual property rights. The use, or possession, of unlicensed copies or "pirated" versions of software is illegal and is expressly prohibited under the Copyright Designs and Patents Act and Great Oaks Small School policy

10. I have read and understood the school's Online Safety (including Social Media) policy which covers the requirements for use of mobile phones and personal devices and safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of learners within the classroom and other working spaces..

11. I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of to the Designated Safeguarding Lead (Julie Kelly) or Deputy Designated Safeguarding Leads (Rebecca Taylor, Andy Crane and Kerri Baker) .

12. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, I will report this to the Head Teacher/IT Manager as soon as possible.

13. My electronic communications with current or past students, parents/carers and other professionals will take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.

    - All communication will take place via school approved communication channels, such as a school provided email address or telephone number, and not via my personal devices or communication channels, such as personal email, social networking or mobile phones.

    - Any pre-existing relationships or situations that may compromise this will be discussed with the Designated Safeguarding Lead (Julie Kelly, Head Teacher).

14. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming and any other devices or websites.

    - I will take appropriate steps to protect myself online as outlined in the Online Safety Policy (including Social Media) and will ensure

that my use of IT and the internet will not undermine my professional role, interfere with my work duties and will be in accordance with the Behaviour Policy for Staff and the Law.

15. I will not create, transmit, display, publish or forward any material online that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

16. I will promote online safety with the students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

17. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the Designated Safeguarding Lead (Julie Kelly, Head Teacher).

18. I understand that my use of the school information systems, including any devices provided by the school, including the school internet and school email, may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

19. I understand that the school may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance. Where it believes unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour may be taking place, the school may invoke its disciplinary procedures. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

20. Great Oaks Small School must comply with all UK legislation with respect to the use of ICT. In using Great Oaks Small School facilities you must comply with the following Acts and may be held personally liable for any breach of current legislation as listed below and any future legislation that may be enacted:

- General Data Protection Regulation (GDPR) (EU) 2016/679
- Copyright Designs and Patents Act 1988

- Computer Misuse Act 1990
- Obscene Publications Act 1959
- Freedom of Information Act 2000
- Data Protection Act 2018

Part 2: Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the schools' boundaries and requirements when using the school Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list and all members of the school community are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

1. The school provides Wi-Fi for the school community and allows access for educational use only for students. Limited personal use is provided to staff. All internet/Wi-Fi use is monitored with respect to the schools Online Safety (including Social Media) Policy and Data Protection Policy

2. I am aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The School takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the School premises that is not the property of the School.

3. The use of ICT devices falls under Great Oaks Small School's Acceptable Use Policy, Online Safety (including Social Media) Policy, Behaviour Policy for Staff, Behaviour Policy for Students, Data Protection Policy (and related policies) and Child Protection Policy which all students, staff, visitors and volunteers must agree to and comply with.

4. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

5. School owned information systems, including Wi-Fi, must be used lawfully; 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.

6. I will take all practical steps necessary to make sure that any equipment connected to the schools' service is adequately secure, such as up-to-date anti-virus software, systems updates.

7. The school's wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.

8. The school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school's wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

9. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.

10. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.

11. I will not attempt to bypass any of the schools' security and filtering systems or download any unauthorised software or applications.

12. My use of school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

13. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

14. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (Julie Kelly, Head Teacher) as soon as possible.

15. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead (Julie Kelly, Head Teacher.

16. I understand that my use of the school Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

Designated/Responsible Staff Identified
Julie Kelly, Head Teacher - Designated Safeguarding Lead
Rebecca Taylor - Deputy DSL
Andy Crane - Deputy DSL
Kerri Baker - Deputy DSL
Mark Cornwell – IT Manager

Other Related Policies	**Date**	**Supporting Documents**	**Date**
Image Use Policy		General Data Protection Regulation (GDPR) (EU) 2016/679	2016
Online Safety Policy (including Social Media)		Copyright Designs and Patents Act 1988	1988
Behaviour Policy for Staff		Computer Misuse Act 1990	1990
Data Protection Policy		Obscene Publications Act 1959	1959
Behaviour Policy for Students		Freedom of Information Act 2000	2000
Child Protection Policy		Data Protection Act 2018	2018
		Acceptable Use Policy Staff Resources	current

Version Number	**Purpose/Change**	**Author**	**Date Changed**	**Review Date**
2.0	Review & updated	JUDICIUM KELSI Rebecca Taylor	April 2019	April 2020
2.1	Amendment added regarding virus scanning of removable devices on page 3 (Part 1 point 4.)	Mark Cornwall & JK	26 April 2019	April 2020