

(SAFEGUARDING & DATA PROTECTION)

ACCEPTABLE USE POLICY FOR VISITORS & VOLUNTEERS 2.0

HEAD TEACHER: JULIE KELLY

CHAIR OF TRUSTEES: CLIVE BEST

Date Agreed: April 2019

Date of Next Review: April 2020

ACCEPTABLE USE POLICY FOR VISITORS & VOLUNTEERS 2.0

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

Acceptable Use Policy for Visitor/Volunteer

NB For visitors/volunteers and staff who do not access school/setting ICT systems

As a professional organisation with responsibility for children's safeguarding it is important that all members of the community, including visitors and volunteers, are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy.

This is not an exhaustive list; visitors/volunteers are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. Visitors and volunteers must ensure that any personal data of learners, staff or parents/carers is kept in accordance with Data Protection legislation, including GDPR. Any data which is being removed from the site, such as via email or on memory sticks or CDs, will be encrypted by a method approved by the setting. Any images or videos of learners will only be used as stated in the school image use policy and will always reflect parental consent.
2. Visitors and volunteers must read and understand 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.
3. Visitors and volunteers must follow the school's policy regarding confidentiality, data protection and use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.
4. Visitor and volunteer electronic communications with students, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
 - o All communication will take place via school approved communication channels such as via a school provided email address or telephone number and not via personal devices or

ACCEPTABLE USE POLICY FOR VISITORS & VOLUNTEERS 2.0

- communication channels such as via 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).
5. Visitor and volunteer use of ICT and information systems will be compatible with their role within school. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. Visitors and volunteers must take appropriate steps to protect themselves online and their use of ICT will not interfere with their work duties and will always be in accordance with the school AUP and the Law.
 6. Visitors and volunteers must 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 their professional role, the school into disrepute.
 7. Visitors and volunteers will promote online safety with the children in their care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
 8. If Visitors and volunteers have any queries or questions regarding safe and professional practise online either in school or off site, they must raise them with the Designated Safeguarding Lead (Julie Kelly, Head Teacher).
 9. Visitors and volunteers will report any incidents of concern regarding children's online safety to the Designated Safeguarding Lead (Julie Kelly, Head Teacher) or Deputy Designated Safeguarding Leads (Rebecca Taylor, Andy Crane, Kerri Baker) as soon as possible.
 10. Visitors and volunteers must understand that if the school believes inappropriate use or unacceptable behaviour is taking place, the school may invoke its disciplinary procedure. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.
 11. Great Oaks Small School must comply with all UK legislation with respect to the use of ICT. In using Great Oaks Small School facilities visitors and volunteers 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

ACCEPTABLE USE POLICY FOR VISITORS & VOLUNTEERS 2.0

- Freedom of Information Act 2000
- Data Protection Act 2018

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. 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, Staff Behaviour Policy, Student Behaviour Policy, 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; visitors and volunteers must 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.

ACCEPTABLE USE POLICY FOR VISITORS & VOLUNTEERS 2.0

6. Visitors and Volunteers must 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 visitor and volunteer's own risk. By using this service, visitors and volunteers acknowledge that security errors and hacking are an inherent risk associated with any wireless network.
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 visitors or volunteers sole responsibility; and visitors and volunteers will indemnify and hold harmless the school from any such damage.
9. The school accepts no responsibility regarding the ability of equipment, owned by visitors and volunteers, to connect to the school's wireless service.
10. Visitors and volunteers must respect system security and not disclose any password or security information that is given to them. To prevent unauthorised access, visitors and volunteers will not leave any information system unattended without first logging out or locking their login as appropriate.
11. Visitors and volunteers must not attempt to bypass any of the schools' security and filtering systems or download any unauthorised software or applications.
12. Visitors and volunteers use of school Wi-Fi should 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. Visitors and volunteers must 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. Visitors and volunteers 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.

ACCEPTABLE USE POLICY FOR VISITORS & VOLUNTEERS 2.0

15. If visitors and volunteers have any queries or questions regarding safe behaviour online, they should discuss them with the Designated Safeguarding Lead (Julie Kelly – Head Teacher).
16. Visitors and volunteers must understand that their 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