Statutory

On-line Safety

Acceptable Use Policy including Network Security

(for staff, governors and visitors)

These rules are designed to protect staff and visitors from on-line safety incidents and promote a safe on-line learning environment for staff and pupils. Through the policy the above are referred to as "staff". All staff must read and sign the Acceptable Use Policy before using any school ICT resource.

This policy aims to:

- Promote the professional, ethical, lawful and productive use of the School's ICT systems and infrastructure;
- Define and identify unacceptable use of the School's ICT systems and external systems;
- Educate users about their data security responsibilities;
- Describe why monitoring of the ICT systems may take place;
- Define and identify unacceptable use of social networking sites and school devices; and
- Specify the consequences of non-compliance.

The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the School's Data Protection Policy for further information.

If you are in doubt and require clarification on any part of this document, please speak to Jane Gammell, Network Manager and GDPR Lead.

Your school mobile device, laptop/chromebook/ipad is on loan to you while you remain employed by Oak Green School. No personal equipment should be connected to or used with the School's ICT systems.

The Network Manager is responsible for purchasing and/or allocating ICT equipment to individuals. Individual laptops/desktop computers or ICT equipment may be removed at any time and without prior warning for regular maintenance, reallocation or any other operational reason. Maintenance includes but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

Whilst in your possession, the following points should be adhered to:

1. The device remains the property of Oak Green School and is only for the use of the member of staff to whom it is issued. It must be returned to the School in an acceptable condition if requested by the Network Manager or Co-Headteachers or if the member of staff leaves their post (temporary or permanently). Google Drive should be used if additional storage is required.

2. Laptops may be taken off the premises but staff should be aware that the school Insurance does not cover these devices when they are out of school. Please make every effort to keep devices secure; do not leave unattended in cars or public places. Trip iPads which have strong passcodes are available for staff to take offsite when going on a school outing. Only school owned devices will be used to take photographs of pupils.

3. When any computer is left unattended either in school or in another location it must either be logged off or locked to protect any data breaches or unauthorised access to the network.

4. Any loss of laptop or other storage devices known or suspected to contain sensitive information should be reported to the School's GDPR Lead immediately.

5. Staff are responsible for ensuring the operating system software on their device is kept up to date by installing updates and patches within 14 days of being notifed. The Network Manager will notify staff on a regular basis when these updates become available.

6. Only software previously installed on the laptop computer may be used. External agency or support services are not permitted to tamper with school laptop hardware or download software or third party applications without the consent of the Network Manager.

7. Anti-virus software is installed on school laptops and pcs and should be checked by staff regularly to ensure there are no issues which need reporting to the Network Manager. The Network Manager is available to support this task if staff require help.

8. Any faults with laptops must be reported to the Network Manager so they can be resolved as soon as possible. Staff should not attempt to repair faults. Staff will be responsible for the repair and maintenance costs of laptops (hardware and software) necessary due to negligence or misuse.

10. Training in accessing the network and general data housekeeping will be provided.

11. Staff are reminded that any charges incurred by accessing the Internet from home are not chargeable to the school.

12. The school's internet, email, computers, laptops and mobile technologies will be used for business purposes only as required by staff's professional role.

13. All users of the ICT systems at the School must first be registered. Following registration, a network user account will be created consisting of a username, password and an e-mail address. All user account details are for the exclusive use of the individual to whom they are allocated.

14. Laptops and school accounts should have a strong password containing special characters and numbers. Passwords can be checked to see if they have been compromised by visiting *www.haveibeenpwned.com* and should be changed immediately if there is the possibility they have been compromised. Passwords should not be re-used. Users must take all reasonable precautions to protect their user account details and must not share them with any other person, except to designated members of the Network Security Team for the purposes of system support.

15. All users are personally responsible and accountable for all activities carried out under their user account(s). Users must report any security breach or suspected breach of their network, email or application account credentials to the Network Manager as soon as possible. Users should only access areas of the School's computer systems to which they have authorised access.

16. When accessing school emails or software such as BROMOM, CPOMS, Medical Tracker and any assessment software that contain any other sensitive information relating to Oak Green School, staff will ensure that it is conducted on a device that has the appropriate security measures and logged out after each use. There are times when it may be necessary to access school emails on personal devices and these devices should be biometrically, pin or password protected. Emails should not contain children's full names in the subject line or the main body of the text. Initials and Class number should be used wherever possible.

17. The Network Manager should be notified as soon as possible if any emails received are believed to be phishing attacks.

18. It is possible that some uncategorised websites for educational use may be blocked by the Firewall. In this instance these should be reported to the Network Manager.

19. Personal information and contact details must not be shared with pupils or parents. Business emails will only be sent using a nominated school email address. Personal email addresses are not to be used.

20. Any online communications with staff, parents, governors or other professionals are to be compatible within the professional role held and all written communications with parents are to be presented on headed paper. Where possible, emails must not contain personal opinions about other individuals e.g., other staff members, children or parents.

21. Whilst using school devices staff should not browse, download, upload or distribute any material which could be considered offensive, illegal or discriminatory.

22. Staff will refrain from carrying out any personal purchasing on school owned computers and will respect copyright and intellectual property rights. Staff will refrain from downloading any material for personal use whilst connected to the school's wireless network.

23. Personal devices in school will only be used when on non-contact time and not in any location where children are present. Personal mobile devices will be kept in a secure location whilst in school, out of sight and switched to silent. This includes the use of Smartwatches. Smartglasses or glasses with recording capability are not to be worn on the school site.

24. User accounts for members of staff/students/governors that have left Oak Green will be immediately disabled and removed at the earliest opportunity.

25. Where practical multi-factor authentication will be provided for sensitive data and cloud based services.

26. Firewall monitoring logs will be checked to aid in detecting suspicious activity and users will be advised if their browsing history is a cause of concern for network security.

27. Staff will promote on-line safety with pupils in their care and will help them to develop a responsible attitude to systems use and to the content they access or create. Any websites that are planned for children to access will be thoroughly checked for content and pupils using the internet will be supervised at all times.

28. Images of pupils will only be taken on school devices and used for professional purposes in line with school policy with consent of the parent or carer. Images will not be distributed outside of school without the permission of the parent/carer and Head Teacher. No information on individual children, including photographs, should be stored on the laptop hard drive. This information should be stored ONLY on the staff drive on the schoolshare network and images deleted on a regular basis.

29. Staff will not upload any media, including photographs or videos, of pupils (not related to them or part of a family group) to any personal social networking sites and will report any befriending requests on social media, electronic messaging or personal emails from current or ex parents or pupils.

30. Staff will ensure that their personal use of social media is compatible with their professional role and does not bring the school into disrepute. This policy should be read in conjunction with the Schools Online Safety including Filtering and Monitoring Policy, Social Media and Networking Policy, Mobile Phones, Personal Devices and Imaging Policy and Artificial Intelligence and Machine Learning Policy for Staff.

31. In line with the school's safeguarding responsibilities any on-line safety concerns must be reported via the School's Safeguarding reporting tool, CPOMS, so that the designated safeguarding officers are alerted as soon as possible.

32. Where evidence of misuse of school devices, the school network or the internet is found, the School may undertake a more detailed investigation. The School reserves the right to audit and/or suspend a user's network access, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

Acceptable Use Policy including Network Security

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

If necessary, such information may be handed to the police in connection with a criminal investigation.

As a user of the school network resources I confirm that I have read and understood the contents of this User Agreement and agree to follow the rules as set out in the Agreement.

I confirm I will use the network/equipment in a responsible way and observe all the restrictions explained in the School Acceptable Use Policy. If I am in any doubt, I will consult the Network Manager.

I agree to report any issues with any school owned electronic resources to the Network Manager as soon as possible.

I agree to report any misuse of the network, any websites which appear suspicious, contain inappropriate material, any comments/uploads to any social media platforms that may bring the school into disrepute or are of a defamatory nature.

I agree to ensure that portable equipment such as iPads or laptops will be kept secured when not in use and passwords kept confidential.

If I do not comply with the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action.

I agree that my use of a personal device, i.e. phone, smartwatch will only be used as agreed in areas where there are no children.

Name ……

Signed ……

Date ……

For new members of staff please sign, copy and return this page for school records.