Oakwood Infant and Nursery School

IT Usage Policy (OAK002/07/2022)

School Mission Statement

At Oakwood Infant and Nursery School we provide a safe, healthy, happy and creative learning environment for everyone, through high expectations and mutual respect.

We are all stars, watch us shine.

Reviewed: 15.7.2021
Approved: 15.2.2021
To be reviewed: 15.7.2022

Use of computers, email and the internet

The email system and the internet/intranet can be extremely valuable tools in an educational context, encouraging the development of communication skills, and transforming the learning process by opening up possibilities that, conventionally, would be impossible to achieve.
The use of electronic mail as a medium for paper mail replacement and as a means of enhancing communications is encouraged.

Those using the school's electronic mail services and/or the internet are expected to do so responsibly and to comply with all applicable laws, policies and procedures, and with normal standards of professional and personal courtesy and conduct.
Those using their own personal computer or equipment for school purposes must only do so where this has been authorised by management. Whilst using their own computer for school purposes, employees must do so responsibly and to comply with all applicable laws, policies and procedures, including the provisions set out in this Policy.

Employees should not bring their own computer or equipment onto school premises unless this has been specifically authorised by an appropriate manager. In such circumstances, the computer/equipment must be kept securely (at the risk of the employee) and security protected so that it cannot be accessed by pupils at the school.

Any personal use of such equipment must be restricted to an employee's break times or outside their normal working hours and must not impact on their duties in any way. Any personal equipment which has been authorised in school must have adequate virus protection to protect school systems.

Computers and laptops loaned to employees by the school are provided to support their professional responsibilities and employees must notify their employer of any significant personal use (see 7.1 below). Reasonable access and use of the internet/intranet and email facilities is also available to recognised representatives of professional associations' i.e. union officers.

Employees must not use school equipment or property for personal gain or fraudulent, malicious, illegal, libellous, immoral, dangerous, offensive purposes. Employees should not undertake IT related activities that are contrary to the school's policies or business interests including accessing, downloading, storing, creating, copying or distributing offensive material (this includes but is not limited to pornographic, sexual, violent or criminal content and racist, sexist, or otherwise discriminatory material).

All forms of chain mail are unacceptable and the transmission of user names, passwords or other information related to the security of the school's computers is not permitted.

7.1 Personal Use

7.1.1 The school's e-mail and internet service may be used for incidental personal purposes, with the approval of the line manager, provided that it:

- does not interfere with the school's operation of computing facilities or email services;
- does not interfere with the user's employment or other obligations to the school;
- does not interfere with the performance of professional duties;
- is of a reasonable duration and frequency;
- is carried out in the employees break times or outside their normal working hours;
- does not over burden the system or create any additional expense to the school;
- does not bring the school and its employees into disrepute.

Such use must not be for:

- unlawful activities;
- commercial purposes not under the auspices of the school;
- personal financial gain;
- personal use that is inconsistent of other school policies or guidelines.

If an employee fails to meet these conditions for personal use, their rights to use equipment may be withdrawn. If an employee fails to follow this policy and other supporting procedures, this could result in disciplinary action.

7.1.2 Use of email and internet at home

Access to the internet from an employee's home using a school owned computer or through
school owned connections must adhere to all the policies that apply to their use. Family members or other non-employees must not be allowed to access the school's computer system or use the school's computer facilities, without the formal agreement of their line manager.

7.2 Security

7.2.1 The school follows sound professional practices to secure email records, data and system programmes under its control. As with standard paper based mail systems, confidentiality of email cannot be 100% assured. Consequently users should consider the risks when transmitting highly confidential or sensitive information and use the appropriate level of security measure.

7.2.2 Enhancement of the base level security to a higher or intermediate level can be achieved by the use of passwords for confidential files. It should be remembered emails forwarded from another individual can be amended by the forwarder. This possibility should be considered before acting on any such mail.

7.2.3 In order to effectively manage the email system, the following should be adhered to:

- open mailboxes must not be left unattended;
- care should be taken about the content of an email as it has the same standing as a memo or letter. Both the individual who sent the message and/or the school can be sued for libel;
- reporting immediately to IT units when a virus is suspected in an email.
- All devices such as phone's, laptop's and tablets must be encrypted
- All passwords must be 8 characters or more including capitals, lower case letters, numbers and special characters
- Passwords must be changed every 60 days

7.3. Privacy

7.3.1 The school respects users' privacy. Email content will not be routinely inspected or monitored, nor content disclosed without the originator's consent. However, under the following circumstances such action may be required:

- when required by law;
- if there is a substantiated reason to believe that a breach of the law or school's policy has taken place;
- when there are emergency or compelling circumstances.

7.3.2 The school reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other policies.

Employees will be notified of any monitoring which will take place and the reason for it. Employees will also be notified of what information will be recorded and retained, and for how long, and who will have access to the information. If monitoring takes place, the school will also notify employees of how such information will be used, which will include using such information for disciplinary purposes where applicable. Employees may make representations about any such monitoring,
Monitoring will be reasonable and in accordance with Data Protection and Human Rights obligations.
7.3.3 Employees should not have any expectation of privacy to his or her use of the school
systems (including but not limited to networks/servers/internet usage/networks/wi-fi). The school reserves the right to inspect any and all files stored in computers or on the network in order to assure compliance with this policy. Auditors must be given the right of access to any document, information or explanation that they require.

7.3.4 Use of the employee's designated personal file area on the network server provides
some level of privacy in that it is not readily accessible by other members of staff. These file areas will however be monitored to ensure adherence to policies and to the

law. The employee's personal file area is disk space on the central computer allocated to that particular employee. Because it is not readily accessible to colleagues it should not be used for the storage of documents or other data that should be open and available to the whole staff or wider school community.

7.3.5 Managers will not routinely have access to an employee's personal file area. However,
management information on usage size of drives or a report outlining the amount of information held on an individual's personal file area will be made available from time to time.

7.4. Email/IT Protocols

A good practice guide for employees on the use of emails is available during GDPR training which is provided to employees annually.

7.4.1 Users must:

- within working hours, respond to emails in a timely and appropriate fashion. The system is designed for speedy communication. If urgent, the email requires a prompt response, otherwise a response should be sent within a reasonable timeframe according to the nature of the enquiry;
- not use anonymous mailing services to conceal identity when mailing through the Internet, falsify e-mails to make them appear to originate from someone else, or provide false information to any Internet service which requests name, e-mail address or other details;
- not abuse others (known as 'flaming'), even in response to abuse directed at themselves;
- not use electronic media and services in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system;
- not use, transfer or tamper with other people's accounts and files;
- not use their own equipment to connect to the School's network unless specifically permitted to do so and the equipment meets appropriate security and other standards.

Under no circumstances is personal equipment containing inappropriate images or links to them, to be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work in a school or with children.

- Ensure that pupils are not exposed to any inappropriate images or web links whether on school owned computers or on their own computer/equipment used for school purposes (where this has been authorised). School/service and adults need to ensure that internet equipment used by children have the appropriate controls with regards to access. E.g. personal passwords should be kept confidential.
- not store sensitive or confidential data on their own equipment – this extends to personal cameras, mobile phones and other similar devices;

- use unsecured disks/memory sticks (all disks/memory sticks used must be encrypted and/or password protected);
- respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner;
- not use the internet/intranet facilities or equipment to deliberately propagate any virus, worm, Trojan horse or any such other programme that is harmful to normal computer operations;

If a user finds themselves connected accidentally to a site that contains sexually explicit or offensive material, they must disconnect from that site immediately. Such unintentional access to inappropriate internet sites must be reported immediately to their line manager. Any failure to report such access may result in disciplinary action.

7.4.2 Except in cases in which explicit authorisation has been granted by an appropriate manager, employees are prohibited from engaging in, or attempting to engage in:

- monitoring or intercepting the files or electronic communications of other employees or third parties;
- hacking or obtaining access to systems or accounts they are not authorised to use;
- using other people's log-ins or passwords;
- breaching, testing, or monitoring computer or network security measures;
- interfering with other people's work or computing facilities;
- sending mass e-mails without consultation with the Head teacher. Global sends (send to every Board in the Global address book) are prohibited;

7.5. Data Protection

7.5.1 General Data Protection Regulations 2018 prohibits the disclosure of personal data except in accordance with the principles of the Regulations. This prohibition applies to e-mail in the same way as to other media. Information gathered on the basis that it would be seen by specified employees must not be given to a wider audience. In accordance with the provisions of Article 8 of the European Convention on Human Rights, the school respects the right to privacy for employees who use IT equipment but does not offer any guarantee of privacy to employees using IT equipment for private purposes.
7.5.2 As data controller, the school has responsibility for any data processed or stored on any of its equipment. Any employee monitoring will be carried out in accordance with the principles contained in the Code of Practice issued by the Information Commissioner under the provisions of the General Data Protection Regulations 2018.

7.5.3 In order to comply with its duties under the Human Rights Act 1998, the school is required to show that it has acted proportionately, i.e. are not going beyond what is necessary to deal with the abuse and that the need to investigate outweighs the individual's rights to privacy, taking into account the school's wider interests. In drawing up and operating this policy the school recognises that the need for any monitoring must be reasonable and proportionate.

7.5.4 Auditors (internal or external) are able to monitor the use of the school's IT equipment and the storage of data. They are nevertheless bound by the provisions of the Human Rights Act 1998, the General Data Protection Regulations 2018, associated codes of practice and other statutory provisions and guidance, including the Regulation of Investigatory Powers Act 2000 in respect of any activity that could be classed as directed surveillance.

7.5.5 Any breach of this policy by individuals will be dealt with in regard to the schools Disciplinary and Dismissal Policy.

7.5.6 All members of staff, volunteers and governors will be asked to sign an agreement regarding this policy included in the Staff Induction Pack on an annual basis.

7.5.7 Please see Induction Pack – Agreement Part 3 regarding Social Media