ICT Guidelines

Legislation

- Data Protection Act 2018
- General Data Protection Regulation (Regulation (EU) 2016/679)

Related Policies

- Whistleblowing
- Social Networking
- Safeguarding Children/Child Protection
- Online Safety

This Policy describes the rights and responsibilities of staff using resources, such as computers, tablets, the internet, landline and mobile telephones, and other electronic equipment. It explains the procedures you are expected to follow and makes clear what is considered acceptable behaviour when using them. These devices are a vital part of our business and should be used in accordance with our policies in order to protect children, staff and families.

ICT Guidelines Networked resources, including internet access, are potentially available to staff and children in the school. All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and/or retrospective investigation of the user's use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter. These networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. Any expression of a personal view about Little Discoverers matters in any electronic form of communication must be endorsed to that effect. Any use of the network that would bring Little Discoverers into disrepute is not allowed. Little Discoverers expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to children in the use of such resources. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Conditions of use

Personal responsibility Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to member of staff responsible.

Acceptable use

Users are expected to utilise the network systems in a responsible manner. It is not possible to set a complete set of rules about what is and what is not acceptable but the pages on network etiquette and privacy together with unacceptable use provides some guidelines on the matter.

Network Etiquette and privacy

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

- Be polite – never send or encourage others to send abusive messages.
- Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
- Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
- Privacy – do not reveal any personal information (for example home address, telephone number) about yourself or other users. Do not trespass into other users' files or folders.
- Password – do not reveal your password to anyone. If you think someone has learned your password then contact member of staff responsible.
- Electronic mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.
- Disruptions – do not use the network in any way that would disrupt use of the network by others.
- Staff finding unsuitable websites through the school network should report the web address to the member of staff responsible.
- Do not introduce memory sticks into the network without having them checked for viruses.
- Do not attempt to visit websites that might be considered inappropriate. Such sites would include those relating to illegal activity. Downloading some material is illegal and the police or other authorities may be called to investigate such use.
- Unapproved system utilities and executable files will not be allowed to be attached to email.
- Files held on the school's network will be regularly checked by the member of staff responsible.
- It is the responsibility of the user (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this policy document, and to ensure that unacceptable use of the internet. Examples of unacceptable use include but are not limited to the following:

Unacceptable use

- Users must log in with their own user ID and password, where applicable, and must not share this information with other users. They must also log off after their session has finished.

- Users finding machines logged on under other user's username should log off the machine whether they intend to use it or not.
- Accessing or creating, transmitting, displaying or publishing any material (for example images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety. There are filters in place to block emails containing language that is or may be deemed to be offensive.
- Accessing or creating, transmitting or publishing any defamatory material.
- Receiving, sending or publishing material that violates copyright law. This includes through video conferencing and web broadcasting.
- Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data.
- Transmitting unsolicited material to other users (including those on other networks).
- Unauthorised access to data and resources on the school network system or other systems.
- User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.
- **Additional guidelines**

- Users must comply with the acceptable use policy of any other networks that they access.
- Users must not download software without approval.
- **Media publications** Named images of pupils (for example in photographs, videos, web pages) must not be published under any circumstances. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- **Wilful damage** Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.
- **Physical security** Staff users are expected to ensure that portable ICT equipment such as laptops, digital still and iPads are securely locked away when they are not being used. No iPads, laptops or memory sticks should ever be left vulnerable to theft e.g. left in unattended car.
- **Network security** Users are expected to inform member of staff responsible immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must log in with their own user ID and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network.
- **Services** There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service

interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

Security and passwords

All electronic devices will be password protected and passwords will be updated on a regular basis. Passwords for our systems are confidential and must be kept as such. You must not share any passwords with any other person; in particular you must not allow any other staff member to know or use our password.

Email

We expect all staff to use their common sense and good business practice when using email. As email is not a totally secure system of communication and can be intercepted by third parties, external email should not normally be used in relation to confidential transactions.

Emails must not be used to send abusive, offensive, sexist, racist, disability-biased, sexual orientation based or defamatory material, including jokes, pictures or comments which are potentially offensive. Such use may constitute harassment and/or discrimination and may lead to disciplinary action up to and including summary dismissal. If you receive unwanted messages of this nature, you should bring this to the attention of your Manager.

Internet access

You must not use the internet facilities to visit, bookmark, download material from or upload material to inappropriate, obscene, pornographic or otherwise offensive websites. Such use constitutes misconduct and will lead to disciplinary action up to and including summary dismissal in serious cases.

Each employee has a responsibility to report any misuse of the internet or email. By not reporting such knowledge, the employee will be considered to be collaborating in the misuse. Each employee can be assured of confidentiality when reporting misuse.

Personal use of the internet, email and telephones

Any use of our electronic communication systems (including email, internet and telephones) for purposes other than the duties of your employment is not permitted.

Emergency personal calls need to be authorised by the manager and where possible, be made on your own personal mobile phone outside the nursery.

Disciplinary action will be taken where:

- the privilege of using our equipment is abused; or
- unauthorised time is spent on personal communications during working hours.

Data protection

When using any of our systems employees must adhere to the requirements of the General Data Protection Regulation 2018 (GDPR). For more information see our Data Protection and Confidentiality Policy.

Downloading or installing software

Employees may not install any software that has not been cleared for use by the manager onto our computers or systems. Such action may lead to disciplinary action up to and including summary dismissal in serious cases.

Using removable devices

Before using any removable storage media which has been used on hardware not owned by us (e.g. USB pen drive, CDROM etc.) the contents of the storage device must be virus checked.

Removable devices must not be taken home unless under exceptional circumstances and authorised to do so by the management team, with prior written permission and risk assessment in place.

Reviewed: August 2024