



IT POLICY

OBJECTIVE

To explain the use of IT equipment and software and the etiquette to be followed for its use. This policy should be applied in conjunction with the Social Networking and Confidentiality Policies.

PERSONAL USE

Equipment owned by and software registered to York Childcare (YC) may only be used for personal use in specific circumstances where prior authority has been obtained from the setting manager eg where the employee is undergoing training.

USING IT EQUIPMENT WITH CHILDREN

It is intended that children will have access to IT equipment to use for games and learning opportunities.

Children should be encouraged to handle IT equipment with care and respect.

Children must never be left unsupervised while watching films, programmes or clips and must not be left unsupervised with access to the internet.

Watching films, programmes or clips is usually a group activity in a nursery or school – children need to be encouraged, over a period of time to develop the skills required to enable them to watch as part of a group, rather than alone.

Monitors playing films will never be left on as a 'back-ground' to other activities; they will be used for a specific purpose and then switched off.

The length of time for which children will be given opportunity to watch films, programmes or clips will be at the discretion of the Room Manager, bearing in mind the age of the children, their level of concentration, interest in the programme and other activities taking place. These factors will be assessed at frequent intervals.

Watching films, programmes or clips will never be a compulsory activity for nursery children – there will always be interesting alternative activities available.

Staff will ensure that all films, programmes or clips are suitable for young children to watch.

Children will be given the opportunity to watch themselves participating in nursery activities on film clips at times, made by nursery staff.

CONFIDENTIALITY ISSUES

The organisation is registered under the Data Protection Act. When issuing or sharing information each employee must ensure that in so doing they are not in breach of that act or of any GDPR requirements. All commercial information must be treated as highly confidential and not to be released unless previously agreed with the Management Board. Information relating to parents and children may only be released to the relevant authorities with the prior permission of the General Manager, CEO or another senior manager.

Please also refer to the Data Protection, GDPR, Confidentiality and Social Media Policies.

E-MAIL ADDRESSES

Employees must ensure that business related emails are sent from a professional e-mail address. Each nursery has its own e-mail address to facilitate this. There may be circumstances when it is necessary to set up a new email address for this purpose (eg to link with a social



media account). Guidance on this matter can be obtained from the general office. Passwords to access e-mail accounts must be recorded and kept in a secure place, with copies of the information sent to the General Office.

SENDING E-MAILS

Messages sent by e-mail from YC PC's are for business use. They must be professional at all times as every communication represents the organisation.

If sending e-mails to several recipients, consideration must be given as to whether the circulation list should be available for all to see or whether it should be sent as 'Blind Carbon Copy' (BCC) to maintain confidentiality of other people's email addresses. Circulars to parents MUST be sent using the Blind Carbon Copy (BCC) feature. Any breach of this must be reported as part of our obligations under GDPR. (See GDPR privacy statement information)

DISCLAIMERS ATTACHED TO E-MAILS

All e-mails must have the organisation disclaimer attached as follows:

'This e-mail has been sent from the office of YC Ltd. It may contain information, which is privileged and confidential within the meaning of applicable law. Accordingly, any dissemination, distribution, copying or other use of this message or any of its content by any other person other than the intended recipient may constitute a breach of civil or criminal law and is strictly prohibited. In the event that it has been delivered inadvertently to the incorrect location please either telephone 01904 409763 or e-mail: headoffice@yorkchildcare.co.uk

Viruses: although we have taken steps to ensure that this e-mail and attachments are free from any virus, we advise that in keeping with good computing practice the recipient should ensure they are actually virus free.'

USE OF LANGUAGE AND ETIQUETTE

The organisation policy on salutation is as follows:

At the beginning : Dear xxxxxxxxxxx or just xxxxxxxxxxx

At the end : 'Regards' followed by the employee name in full

'Kind regards' may be used for people you are more familiar with

Please remember that block capitals in e-mails can be regarded as shouting and should be used with care.

E-mails must never be sent in haste; it is important to reflect on their content and phrasing before sending.

Letters and reports are to be formatted in accordance with the organisation standards as set out in the Administration Manual (ie converted to a non-copyable format such as PDF).

If a message is received which has been repeatedly forwarded this should be deleted after reading. YC users should not forward messages in this format but should start a new thread.

A professional communication style is required at all times when communicating by email. There may be exception to this only when the message is a part of an internal conversation thread with colleagues within the organisation.



HOUSEKEEPING PRACTICES

- All PC's and devices which contain personal data or photographs of children must be password protected.
- Where particular documents are confidential then they must be password protected or equivalent protection must be used. A record of all passwords is to be kept in a file in the office safe.
- All laptops must be switched off at night unless planned maintenance (eg de-fragmenting) is in progress.
- Tablets and laptops must be stored in a locked room or cabinet overnight.
- All IT equipment must be handled with care and looked after in accordance with manufacturers instructions.
- When staff take a break from their work then they are expected to ensure that their PC is placed on standby to maintain confidentiality and to avoid time-wasting in the accidental erasure of the document on which they had been working.
- Staff are expected to download updates as required to promote the efficiency of the running system on the PC and to ensure the ongoing security of the virus protection system.
- All policy documents or other standard documents must have the relevant date of amendment entered as a footer to ensure that all employees can check that they have the latest version. Previous versions no longer required must be archived in accordance with insurance recommendations.
- An 'out of office notification' must be set at times when no-one will be responding to emails on a daily basis.

PROHIBITION OF INAPPROPRIATE MESSAGES

Messages must not be sent if they might cause offence or harassment.

It is forbidden to send any material, in any format, which the recipient or other person who may come into contact with the message may find objectionable.

This would include material, which is:

- Defamatory
- Offensive, distasteful or obscene
- Untrue or malicious
- Spreads gossip
- Likely to constitute bullying or harassment
- Is in breach of any of YC's policies
- Is of a political nature
- Is in breach of copyright
- Is for personal gain

PROHIBITION OF ACCESSING CERTAIN INFORMATION

Employees are prohibited from deliberately accessing offensive, obscene or indecent material from the Internet, such as pornography, racist or sexist material, violent images, incitement to criminal behaviour etc. If such access occurs accidentally then the incident must be immediately reported to the General Manager who will record it in the IT file.



STORAGE OF DATA

- In storing data, consideration must be given to the sensible use of folder and file naming. It is recognised that the Nurseries, General Office and the OOSSS may have different criteria in this and each section should record their system of naming folders and documents. (Details to be included in the Admin Manual).
- Data stored on the server at the General Office is backed-up automatically every day to cloud-based storage co-ordinated by the company appointed to manage IT matters for YC.
- Backup storage of data held on nursery laptops must be carried out on a regular basis onto an external hard-drive device provided specifically for this purpose which must be stored in a locked cabinet.
- If any data is stored using a portable device such as a memory stick, it is the responsibility of the employee to ensure that the device is kept in a secure place and that the data stored on it cannot be accessed without a password in case it is lost or stolen. No personal data may be stored on a memory stick.

AWARENESS OF LEGISLATION

Legislation exists covering copyright and licensing restrictions. The organisation holds valid licenses for all software installed on the IT equipment. Before installing any further software employees must verify that they are not contravening this legislation. This is particularly important in relation to downloading and forwarding material, whether Internet or e-mail, and including unauthorised software, games, magazine disc items etc. The importation of viruses is often through downloading files and programmes from external sources.

IT PROBLEMS

All IT problems whether hardware or software must be reported the office administrative assistant who will record the details in the IT file. The organisation has one IT firm to whom problems are addressed and the office administrator will either contact that firm or seek authorisation for the employee to contact them. When the problem is resolved the employee must report back to the office administrator with details of how the problem was resolved. If necessary the IT firm must be asked to record the details. In this way it is possible to monitor the reason for problems and to ensure that any caused by inadequate IT knowledge by the employee are resolved by appropriate training.

TRAINING

The organisation intends that all managers and senior staff are appropriately IT trained. Funding will be provided where required for course costs.

All other employees will be provided with appropriate training to ensure that they can complete their duties.

MONITORING

The General Manager is responsible for monitoring the use of IT and will check on the housekeeping practices to ensure they are being followed. The organisation reserves the right to employ IT experts to review the use of IT to ensure no other breaches occur.



IT REPRESENTATIVE

Each setting will appoint a person with sufficient IT knowledge to fulfil the role of IT Representative. This person will have responsibility for the following tasks:

To ensure that:

- an up-to-date inventory of all IT equipment is maintained
- new members of staff are familiarised with the IT and Social Networking policies within one month of starting their job
- routine 'housekeeping and maintenance' is carried out on IT equipment in accordance with this policy
- any IT problems are recorded, passed on to head-office and responded to within a reasonable timescale
- social networking sites are updated on a regular basis (at least weekly)

SOCIAL NETWORKING

Please see separate policy

WEBSITE

YCL has its own website www.yorkchildcare.co.uk

It is the responsibility of senior managers to ensure the website remains up to date and contains accurate information, notifying the business support administrative assistant of any updates which are required.

Photographs of children may only be posted on the website with consent from their parents or guardians and must not show their names.

Managers must ensure that any weblinks to and from the YC website are suitable.

As developments in IT move rapidly, there may be times when this policy needs to be applied flexibly and amended quickly to reflect the advances made in technology.

BREACH OF POLICY

If an employee is found to be in breach of any of the IT regulations, policies or procedures then disciplinary action will follow.