

Stower Vale Pre-school

INTERNET POLICY

The internet is part of everyday life. Knowledge and experience of information and communication technology (ICT) should be considered as essential. Developmentally appropriate access to computers and the internet in the early years contributes significantly to children and young people's enjoyment of learning and development.

Children and young people learn most effectively where they are given managed access to computers and control of their own learning experiences; however such use carries an element of risk. Early years practitioners, their managers and volunteers, alongside parents and carers, should make children and young people aware of the potential risks associated with online technologies. This empowers them with the knowledge and skills to keep safe, without limiting their learning opportunities and experiences.

Aims

- The internet Policy aims to outline safe and effective practice in the use of the internet. It provides advice on acceptable use and effective measures to enable children, young people and adults to use ICT resources in a safer online environment.

Scope

- The Internet Policy applies to all individuals who have access to and/or are users of work related ICT systems. This includes children and young people, parents and carers, early years practitioners and their managers, volunteers, students, committee members, visitors contractors and community users. This list is not exhaustive.
- The Internet Policy applies to internet access through any medium, for example computers, mobile phones and gaming devices.

Responsibility

- It is the responsibility of the Designated Safeguarding Office (DSO) and E-Safety Champion to ensure day-to-day safety issues are implemented, monitored and reviewed. That all ICT users are aware of the procedures to follow in the event of a potentially unsafe or inappropriate incident.

- The DSO and E-Safety Champion at Stower Vale Pre-school will ensure that they attend appropriate training and keep up to date with changes in legislation.
- All ICT users are aware of the procedures that must be followed in the event of a potentially unsafe or inappropriate online incident. This should include the creation of an incident log which should be used to inform future online safety practice.
- All necessary actions are taken to minimise the risk of any identifies unsafe or inappropriate online incidents reoccurring.
- Regular meetings take place with the registered person and senior managers to discuss current issues, review incident reports and filtering/change control logs.
- Effective training and online safety advice is delivered and available to all early years practitioners and their manager and volunteers. This includes advisory support to children, young people, parents and carers as necessary.
- Timely liaison, where appropriate, with other agencies in respect of current online safety practices and the reporting and management of significant incidents.

Further details on the responsibilities of the DSO, early years practitioners and their managers, parents and carers, children and young people are to be found in the Acceptable Use Policy.

Managing online access

Password security:

- Access to Stower Vale Pre-school's laptop which is password secured is only available to the Manager and Deputy Manager.
- The password to the settings laptop will not be shared with any other person.
- If the password has become compromised this must be reported to the Manager immediately.
- Computers and laptops should be set to 'time-out' the current user session if they become idle for an identified period. All ICT users must log-out of their accounts if they need to leave a computer unattended.

Internet Access:

- There is updated and regularly monitored virus protection on all ICT systems with in the setting.
- The setting has secure wireless and broadband settings.
- At Stower Vale Pre-school we have clear Acceptable Use Policy in place together with agreements signed and understood by staff and parents/carers.

- Policies and procedures are reviewed and updated when appropriate legislation is updated or yearly.
- Children at the setting do not have access to the internet at any time.
- Staff mobile phones are not connected to work related ICT systems.
- Effective audit, monitoring and review procedures.
- Secure email accounts.

Online activity should be monitored to ensure access is given to appropriate materials only.

Computers and gaming devices should be sited in areas of high visibility which will enable children, young people and adults to be closely supervised and their online use to be appropriately monitored.

If a child or young person accidentally accesses inappropriate material, it must be reported to an adult immediately. Appropriate action should be taken to hide or minimise the window. The computer should not be switched off, nor the page closed, in order to allow investigations to take place. All such incidents must be reported to the DSO who must ensure a report of the incident is made so that any further actions deemed necessary are taken.

All early years practitioners and their managers should be made aware of the risks of connecting personal mobile devices to work-related ICT systems. Such use will be subject to explicit authorisation by the DSO and will be stringently monitored.

Should it be necessary the download of files or programmes to any work-related system should be effectively managed and monitored.

All users are responsible for reporting any concerns encountered using online technologies to the DSO.

Online Communications

- All official online communications should occur where possible through secure email accounts.
- All online communications are expected to be polite, respectful and non-abusive at all times.
- ICT users are advised not to open emails where they do not recognise the sender or where the format looks suspicious.

When using digital communications, staff and volunteers should:

- Ensure that all communications are transparent and open to scrutiny.
- Not post information online that could bring the group into disrepute.

- Be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

Managing mobile and emerging technologies

- All ICT users will be encouraged to think carefully about the way information can be added and removed from websites by themselves and others.
- Staff at Stower Vale Pre-school adhere to a 'Professional Conduct Agreement' when using social media sites in their own time. The use of such sites must not compromise professional integrity or bring the setting into disrepute.
- Any incidents or suspicions of cyber bullying must be reported to the DSO immediately, please also refer to our Behaviour Policy.
- Emerging technologies can offer potential learning and development opportunities. Their use should be risk assessed before use by children and young people. Where necessary, further training and guidance should be provided to ensure appropriate and safe use of any new technologies.

Linked Policies

- Behaviour Policy
- Acceptable Use Policy
- ICT Misuse Policy
- Camera and Image Policy
- Mobile phone policy
- Safeguarding children