Stower Vale Pre-school

ACCEPTABLE USE POLICY

At Stower Vale Pre-school we understand that the internet has become an integral part of the lives of parents, children and staff in today's society, both within the setting and in their lives outside. The internet and other digital information and communication tools can stimulate discussion and promote creativity helping towards effective learning.

This policy is intended to ensure:

- That children and adults will be responsible users and stay safe whilst using the internet and other communication technologies for educational, personal and recreational use.
- Outline the roles and responsibilities of all individuals who have access to and/are users of, work related ICT systems.
- That Pre-school ICT systems are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Stower Vale Pre-school will ensure that pupils have good access to ICT to enhance their learning and will, in return, expect the staff, committee members and parents/carers to be responsible users.

Scope

The AUP will apply to all individuals who have access to and/or are users of work-related ICT systems. This will include 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.

Parents, carers, and where applicable, other agencies, will be informed of any incidents of inappropriate use of ICT that take place on-site, and, where relevant, off-site

Roles and Responsibilities

Registered person

The registered person has overall responsibility for ensuring that online safety is an integral part of everyday safeguarding practice.
This will include ensuring that:

- Early years practitioners and their managers receive the appropriate training, guidance, time and resources to effectively implement online safety policies and procedures.

- Clear and rigorous policies and procedures are applied to the use/non-use of personal ICT equipment by all individuals who come into contact with the early years setting. Such policies and procedures should include the personal use of work-related resources.
- The AUP is implemented, monitored and reviewed regularly, and that all updates are shared with relevant individuals at the earliest opportunity.
- Monitoring procedures are open and transparent.
- Allegations of misuse or known incidents are dealt with appropriately and promptly, in line with agreed procedures and in liaison with other agencies where applicable.
- Effective online safeguarding support systems are put in place for example filtering controls, secure networks and virus protection.

Designated Safeguarding Officer DSO

The DSO must be a member from the management team who has relevant, current and practical knowledge and understanding of safeguarding child protection and online safety. Access to an individual holding this role would be available at all times, including where necessary the use of a designated deputy.

The DSO will be responsible for ensuring:

- Agreed policies and procedures are implemented in practice.
- All updates, issues and concerns are communicated to all ICT users.
- The importance of online safety in relation to safeguarding is understood by all ICT users.
- The training, learning and development requirements of early years practitioners and their managers are monitored and additional training needs identified and provided for.
- An appropriate level of authorisation is given to ICT users. Not all levels of authorisation will be the same – this will depend on the position, work role and experience of the individual concerned. In some instances, explicit individual authorisation must be obtained for specific activities where deemed appropriate.
- Any concerns and incidents are reported in a timely manner in line with agreed procedures.
- The learning and development of children and young people address online safety
- A safe ICT learning environment is promoted and maintained.

Early years practitioners and their managers

Early years practitioners and their managers will ensure:

- The timely reporting of concerns in relation to alleged misuse or known incidents, subject to agreed procedures.
- ICT equipment is checked before use and all relevant security systems judged to be operational.

- Awareness is raised of any new or potential issues, and any risks which could be encountered as a result.
- Children and young people are supported and protected in their use of online technologies – enabling them to use ICT in a safe and responsible manner.
- Online safety information is presented to children and young people as appropriate for their age and stage of development.
- Children and young people know how to recognise and report a concern.
- All relevant policies and procedures are adhered to at all times and training undertaken as required.

Children and young people

Children and young people should be encouraged to:

- Be active, independent and responsible learners, who contribute as appropriate to policy and review.
- Abide by the Acceptable Use Agreement.
- Report any concerns to a trusted adult.

Parents and carers

Parents and carers should be encouraged to sign Acceptable Use Agreements and to share responsibility for their actions and behaviours.

A copy of an Acceptable Use Agreement should be provided to parents and carers on enrolment of their child at the early years setting. This will be reviewed regularly. It is an expectation that parents and carers will explain and discuss the Acceptable Use Agreement with their child to ensure that it is understood and agreed. Children and young people will also be encouraged to sign the Acceptable Use Agreement alongside their parent carer where appropriate. Records of all signed agreements should be kept on file.

Should parents or carers wish to use personal technologies (such as cameras) within the setting environment, practice must be in line with the setting's policies.

<u>Acceptable use by early years practitioners, their managers and volunteers</u>

Early years practitioners, their managers and volunteers should be enabled to work based online technologies:

- To access age appropriate resources for children and young people.
- For research and information purposes.
- For study support.

All early years practitioners, their managers and volunteers will be subject to authorised use as agreed by the DSO.

All early years practitioners, their managers and volunteers should be provided with a copy of the Acceptable Use Policy and a copy of the

Acceptable Use Agreement, which they must sign, date and return. A signed copy should be kept on file.

Authorised users should have their own individual password to access a filtered internet service provider. Users are not generally permitted to disclose their password to others, unless required to do so by law or where requested to do so by the DSO. All computers are related equipment that can access personal data should be locked when unattended to prevent unauthorised access.

The use of personal technologies is subject to the authorisation of the DSO and such use should be open to scrutiny, monitoring and review.

In the event of misuse by early years practitioners, their manager or volunteers

In the event of an allegation of misuse by an early years practitioner, manager or volunteer, a report should be made to the DSO and/or the registered person immediately, as relevant. Should the allegation be made against the DSO a report should be made to a senior manager or the Committee Chairperson. Procedures should be followed as appropriate, in line with the ICT Misuse Procedure, Safeguarding Policy and/or Disciplinary Procedures. Should allegations relate to abuse or unlawful activity, Children's Social Care, the LADO, Ofsted and/or the Police should be notified as applicable.

Acceptable Use by children and young people

Acceptable Use Agreements are used to inform children and young people of behaviours which are appropriate and others which are deemed unacceptable. This will allow children and young people to take some degree of responsibility for their own actions, understanding the risks and likely sanctions.

The Acceptable Use Agreements are shared and agreed with children and young people and should be displayed as a reminder.

In the event of misuse by children and young people

Should a child or young person misuse ICT, the following sanctions will be applied:

- In the event of deliberate misuse, the parent/carer is informed of the issue. The child or young person may be temporarily suspended from a particular activity.
- Further incidents of misuse, could lead to the child or young person being suspended from using the internet or other relevant technology for an increased period of time. The parent or carer will be invited to

discuss the incident in more detail with a senior manager and the most appropriate course of action will be agreed

- The sanctions for misuse can be escalated at any stage, if considered necessary. In the event that misuse is deemed to be of a serious nature, steps 1 and 2 can be omitted. If a child or young person is considered to be at risk of significant harm, the Safeguarding Policy must also be applied. Allegations of serious misuse will be reported to the most appropriate agency, for example, Children's Social Care.

In the event that 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.

Acceptable use by visitors, contractors and others

All guidelines in respect of acceptable use of technologies must be adhered to by any visitors or contractors.

Linked Policies

- Internet Policy
- Safeguarding Children
- Disciplinary and Grievance Policy
- Camera and image Policy
- Mobile Phone Policy
- Behaviour Policy
- Health and Safety Policy

Attached Procedures

- Online Safety Incident Report Sheet
- Guidance for Reviewing Internet Sites and Recording Log
- Flow Chart for responding to Online Safety Incidents
- Online Safety Incident Log

Stower Vale Pre-school

Where learning through play is fun

Updated to website : 09 February 2016

Online Safety Incident Report Sheet

To be completed as thoroughly as possible by practitioner or manager identifying incident.

Date(s)/times of incident:
Duration of incident: **(e.g. One off, a week, 6 months etc)**
Description of the online safety incident: include details of specific services or websites used (e.g. chat room, instant messenger); email addresses; usernames etc.
Why do you have concerns about this incident?
Has the information been recorded and secured? □ Yes □ No
Has any computer or hardware been secured? □ Yes □ No If yes, who, where, when and what?
Who was involved and how do you know this? Is there any evidence to suggest that false names/details have been given? **Give full details of real names and email addresses etc where known.**

U

Guidance for Reviewing Internet Sites and Recording Log Procedure

Do not follow this procedure if you suspect that the website(s) concerned may contain child abuse images. If this is the case please refer to the Flowchart for responding to line safety incidents and report immediately to the police.

Please follow all steps in this procedure.

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

    - Internal response or discipline procedures
    - Involvement by Local Authority or national/local organisation (as relevant).
    - Police involvement and/or action.

- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the Police would include:

    - Incidents of 'grooming' behaviour.
    - The sending of obscene materials to a child.
    - Isolate the computer in question as best you can. Any change to its state may affect a later Police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the group, possibly the Police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Record of Reviewing Internet Sites

(for suspected harassment/distress)

Group:
Date:
Reason for investigation:

Details of first reviewing person

Group:
Date:
Reason for investigation:

Details of second reviewing person

Group:
Date:
Reason for investigation:

Name and location of computer used for review

Website(s) address	**Reason for concern**

Conclusion and action proposed or taken

Updated to website : 09 February 2016

Stower Vale Pre-school

Where learning through play is fun

Updated to website : 09 February 2016

Stower Vale Pre-school
Where learning through play is fun

Online Safety Incident Log

GROUP:

DATE/TIME	INCIDENT	ACTION TAKEN: WHAT?	ACTION TAKEN: BY WHOM?	INCIDENT REPORTED BY	SIGNATURE

Stower Vale Pre-school

Where learning through play is fun

Updated to website : 09 February 2016