Thanet Early Years Project

E-safety Policy

Thanet Early Years Project (TEYP) recognises that the use of information and communication technologies in early years settings brings great benefits.

We recognise that there can be issues around e-Safety and we plan accordingly to help to ensure appropriate, effective and safer use of electronic communications is implemented.

Why do we need an e-Safety Policy?

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

e-Safety covers issues relating to children and young people as well as adult and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school/nursery. It includes education for all members of the staff on risks and responsibilities and is part of the "duty of care" which applies to everyone working with children.

In order to minimise risks of children accessing inappropriate materials via the internet within our nursery settings, access to the internet is only accessible with adult supervision, and only programmes that are deemed suitable for children under 5 years are accessible. Staff are only able to access the internet with children through the use of interactive white boards (where available).

Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role (see staff code of conduct, E-mail, Social Networking and Internet Policy, IT policy and procedure and TEYP safeguarding children policy).

Breaches of an e-Safety policy can and have led to civil, disciplinary and criminal action being taken against employers and employees. It is crucial that all settings are aware of the offline consequences that online actions can have.

TEYP is aware of their legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit with the Project Manager and the board of Trustees/Directors.

Purpose of the e-Safety policy.

The e-Safety Policy is part of many different TEYP policies including the ICT Policy, Safeguarding Policy, staff code of conduct.

TEYP Designated Safeguarding Lead is responsible for reviewing and updating this policy on an annual basis.

TEYP have a legal responsibility to safeguarding children and staff and this includes online activity.

How can Internet use enhance learning?

The nurseries' Internet access will be designed to enhance and extend young children's learning and development.

Staff guide children to online activities that will support the learning outcomes planned for the pupil's age and ability.

Internet Security

The security of the TEYP information systems and users is reviewed regularly and virus protection is updated regularly.

Personal data sent over the Internet or taken off site will be encrypted.

Portable medial may not be used without specific permission followed by an anti-virus/malware scan.

Unapproved software will not be allowed in work areas or attached to email.

The use of user logins and passwords to access the organisation's network will be enforced.

How will email be managed?

Email is an essential means of communication for staff and managers.

Within TEYP, email should not be considered private and the Project Manager reserves the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of staff and children, and the preservation of human rights, both of which are covered by recent legislation. It is important that staff understand they should be using a work provided email account to communicated with parent/carers and other professionals for any official nursery business. This is important for confidentiality and security and also to safeguard members of staff from allegations (see networking policy).

Staff will only use official TEYP provided email accounts to communicated with parents/carers, other agencies/partners and other TEYP staff, as approved by the Project Manager.

Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter on TEYP headed paper would be.

The forwarding of chain messages is not permitted.

Staff should not use personal email accounts for professional purposes.

Staff should not use their work email for personal use.

How will published contents be managed?

TEYP maintain an organisational website along with a Facebook page.

TEYP take care to ensure no personal information and/or photographs are published without either parent or staff's consent (as appropriate). Images or videos that include children will be selected carefully and will not provide material that could be reused. Children's full names will not be used anywhere on the website, particularly in association with photographs. Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.

The contract details on the website include details of the nurseries and services managed by TEYP along with email addresses of the settings and TEYP Head Office.

The Project Manager will take overall editorial responsibility for online content published by the organisation and will ensure that content published is accurate and appropriate.

Social Networking and social medial sites.

Parents and staff need to be aware that the Internet has emerging online spaces and social networks which allow individually to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

All staff should be made aware of the potential risks of using social networking sites or personal publishing and online dating websites. All TEYP staff receive safeguarding training that covers this.

All staff must be aware of the importance of considering the material they post, ensuring profiles are secured and that publishing unsuitable material may affect their professional status and may result in disciplinary action being taken – see email, social networking and internet policy. Staff should not advertise their place of work on social media - this is covered in Head Office Inductions.

Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiple online gaming, chatrooms, instant messenger and many others.

All members of staff are advised not to public special and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in TEYP IT Policy and Procedure, and Staff Code of Conduct.

When using the internet during working hours to research information relevant to nursery /TEYP, it is important that, in the event staff discover unsuitable sites, they URL must be reported to the Project Manager who will then record the incident and manage the concern as appropriate.

Any material that TEYP believes is illegal must be reported to appropriate agencies such as Kent Police.

How will personal data be protected?

The Data Protection Act 2018 ("the Act") gives individual the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Under the Act, every organisation that processes personal information (personal data) must notify the Information commissioner's office, unless they are exempt.

The Data Protection Act 2018 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individual. The Act sets standards (eight data protection principles) which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individual find out what information is held about them. The eight principles are that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept for longer than is necessary.
- Processed in line with your rights.
- Secure.
- Not transferred to other countries without adequate protection.

TEYP understand their obligations under the Act. For example, with regards to staff employed at TEYP and children who attend our nurseries, personal data will be recorded, processed, transferred and made available in line with the requirements laid down in the Data Protection Act 2018.

For advice and guidance relating to a contravention of the Act, contact the Information Commissioner's Office (ICO) http://www.ico.gov.uk.

Access to the internet within the workplace:

All staff employed by TEYP are informed as part of their induction of the organisation's policies and procedures relating to safer working practices and internet use.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.

Methods to identify, assess and minimise risks will be reviewed regularly.

What to do if incidents of concern arise:

E-safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Any potential concerns must be dealt with at a personal level. Staff are the first line of defence; their observation of behaviour is essential in recognising concerns about children and colleagues and in developing trust so that issues are reported.

It is essential that staff help to develop a safe culture by observing each other's behaviour online and discussing together any potential concerns. Incidents of concern may include unconsidered jokes and comments or inappropriate actions. Any illegal activity would need to be reported to the Designated Safeguarding Lead.

Where there is cause for concern or fear that illegal activity has taken plate or taking place involving the use of computer equipment, TEYP will determine the level of response necessary for the offense disclosed. The decision to involve Police will be made as soon as possible, after contacting the Kent Safeguarding children's board (KSCB) specially if the offence is deemed to be out of the remit of TEYP to deal with.

All staff members are informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.) as part of their induction into post.

The Designated Safeguarding Lead for TEYP will record all reported incidents and actions taken by the organisation in an incident log. Where incidents involve Child Protection concerns, these will then be escalated appropriately.

TEYP will manage e-Safety incidents in accordance with TEYP discipline/behaviour policy where appropriate.

How will e-Safety complaints be handled?

Complaints about Internet misuse will be dealt with under TEYP complaints procedure.

Any complaint about staff misuse will be referred to the Project Manager.

All e-Safety complaints and incidents will be recorded by TEYP including any actions taken.

All members of TEYP staff are reminded about safe and appropriate behaviour online and the importance of not posting any contents, comments, images or videos online which cause harm, distress or offence to any other staff member or service user.

How will Cyber bullying be managed?

Cyber bulling can be defined as “the use of Information Communication Technology, (ICT) particularly mobile phones and the Internet to deliberately hurt or upset someone “DCSF 2007.

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that staff, parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse.

Where bullying outside of the workplace/nursery (such as online or via text) is reported to the Project Manager, it will be investigated and acted on.

Although bullying outside of the work place/nursery (such as online or via text) is reported to the Project Manager, it will be investigated and acted on.

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003 and the Public Order Act 1986. If TYEP staff feel that an offence may have been committed, they should seek assistance from the Police.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provided may be contacted to remove content if the bully refuses or is unable to delete content.
- The Police will be contacted if a criminal offence is suspected.

Mobile phones and personal devices

Mobile phones and other personal devices such as smart watches, games consoles, tablets, PDA’s, and MP3 players etc. are considered to be an everyday item in today’s society and even children in early years settings may own and use person devices to get online regularly. Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internes accesses all common features.

However, mobile phones can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged.
- Their use can render staff subject to cyber bullying;
- Mobile phones with integrated cameras and smart watches could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff.

See mobile phone policy.

e-Safety Contacts and References

CEOP (child Exploitation and Online Protection Centre): www.ceop.police.uk

Online Protection / e-Safety: Sessions House, County Hall, Maidstone Kent ME14 1XQ **03000 41 57 97**

Kent County Council Online Resource https://www.kelsi.org.uk/

Childline: www.childline.org.uk 0800 1111

Childnet: www.childnet.com

Children's Officer for Training and Development https://www.kelsi.org.uk/child-protection-and-safeguarding/safeguarding-training

Digizen: www.digizen.org

Internet Watch Foundation (IWF): www.iwf.org.uk

Kent Police : In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police dial 101.
www.kent.police.uk https://www.kent.police.uk/advice/online-safety

Kent Public Service network (KPSN): www.kpsn.net

Kent Safeguarding Children Board (KSCB): www.kscb.org.uk

Virtual Global Taskforce – Report Abuse: www.virtualglobaltaskforce.com