E-SAFETY STATEMENT

This policy should be read alongside our Child Protection Policy and Safeguarding Policy

Introduction

Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to develop the knowledge and skills our young people will need to access life-long learning and employment.

It is important to recognise the constant and fast paced evolution of technology within our society as a whole. Currently the internet technologies children are using both inside and outside of the classroom include:

- Websites

- E-mail, instant messaging, social media

- Mobile devices with web function – iPads

- Blogs

- Podcasting

Policy, writing and review:

In our setting we understand the responsibility to educate our children on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain safe when using the internet and related technologies, in and beyond the context of the school and to use these technologies responsibly themselves.

Our setting holds personal data on learners, staff and other people to help us to conduct our day-to-day activities.

Everybody in our setting has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling are made aware of the risks and threats and how to minimise them.

Monitoring

All internet activity is logged by the setting's internet provider. These logs may be monitored by the SLT.

Managing e-mail

Our setting gives all staff their own e-mail account to use for all setting business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business.

All e-mails should be written and checked carefully before sending

E-SAFETY STATEMENT

Equal Opportunities

Children with Special Educational Needs:

Staff are aware that all our children fall within this group; but not all, may require additional support, reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a child need support with their social understanding, careful consideration is given to group interactions when raising awareness of e-Safety.

Internet activities are planned and well managed for these children.

E-Safety - roles and responsibilities

As e-safety is an important aspect of strategic leadership within the setting, the Executive Head Teacher has ultimate responsibility to ensure that the policy and practices are embedded and monitored.

All members of the setting have been made aware of their responsibilities concerning e-safety.

E-Safety in our curriculum

Devices and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to our children on a regular basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote e-safety.

Our setting teaches internet skills in many areas of learning as it is embedded across the whole curriculum.

Our setting provides opportunities within a range of learning areas to teach about e-safety.

Key messages about the online risks that children may encounter outside of school and how to keep themselves safe or report incidents are done regularly in areas of learning such as: PSHE or through visits to school by the local community police officers or other organisations.

E-Safety skills development for staff:

Our staff receive regular information and training on e-safety.

New staff receive information on the setting's acceptable use as part of their induction.

All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the setting.

Managing the setting's e-safety messages:

We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.

Any e-safety posters will be prominently displayed.

Managing the internet:

Our setting provides children with supervised access to internet resources through the setting's fixed and mobile internet connectivity.

Staff will preview any recommended sites before use.

All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

All users must observe copyright of materials from electronic resources**.**

Infrastructure

Our setting's internet access is controlled through the LA's web filtering service.

Staff and children are aware that setting based email and internet activity can be monitored and explored further if required.

If staff or children discover an unsuitable site, the screen must be minimized or switched off and the incident reported to the adult working alongside them. This should then be reported immediately to the IT provider, via the school office, who will block it with immediate effect**.**

Parent/carer involvement:

We believe that it is essential for our parents/carers to be promote e-safety both in and outside of school and to be aware of their responsibilities.

Password security:

Password security is essential for staff, particularly as they are able to access and use children's data. Staff are expected to have secure passwords which are not shared with anyone.

Staff are regularly reminded of the need for password security.

Safe use of images - taking of images and film:

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not appropriate to take or store images of any member of the setting community or public, without first seeking consent and considering the appropriateness.

With the written consent of parents (on behalf of children) and staff, the setting permits the appropriate taking of images by staff and children with our setting equipment.