E-Safety Policy
2015-16

FRANCIS ASKEW PRIMARY SCHOOL

E-Safety Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

• Access to illegal, harmful or inappropriate images or other content

• Unauthorised access to / loss of / sharing of personal information

• The risk of being subject to grooming by those with whom they make contact on the internet.

• The sharing / distribution of personal images without an individual's consent or knowledge

• Inappropriate communication / contact with others, including strangers

• Cyber-bullying

• Access to unsuitable video / internet games

• An inability to evaluate the quality, accuracy and relevance of information on the internet

• Plagiarism and copyright infringement

• Illegal downloading of music or video files

• The potential for excessive use which may impact on the social and emotional development and learning of the pupil.

<u>Online sexual harassment</u>

Sexual harassment is likely to: violate a child's dignity, make them feel intimated, degraded or humiliated and/or create a hostile, offensive or sexualised environment.

Online sexual harassment, which might include: non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats.

Any reports of online sexual harassment will be taken seriously, and the police and Children's Social Care may be notified.

Our academy follows and adheres to the national guidance - UKCCIS: Sexting in schools and colleges: Responding to incidents and safeguarding young people, 2016.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

At Francis Askew Primary School we aim to provide the necessary safeguards to help ensure that we have done everything possible to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help pupils (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, governors) who have access to and are users of school ICT systems, both in and out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Teaching and Support Staff are responsible for ensuring that:

• They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices

• They have read, understood and signed the school Staff Acceptable Use Policy

• They report any suspected misuse or problem to the Computing Co-ordinator /Headteacher

• Digital communications with pupils (generic class emails only) should be on a professional level

• E-safety issues are embedded in all aspects of the curriculum and other school activities

• Pupils understand and follow the school E-safety and acceptable use policy

• They monitor ICT activity in lessons, extra-curricular and extended school activities

• They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

• In lessons where internet use is pre-planned pupils should be guided to sites checked for suitability

Our Child Protection co-ordinators are trained in E-safety issues and are aware of the potential for serious child protection issues to arise from:

• Sharing of personal data

• Access to illegal / inappropriate materials

• Inappropriate on-line contact with adults / strangers

• Potential or actual incidents of grooming

• Cyber-bullying

Pupils should:

• Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

• Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school.

The Child Protection co-ordinator and the computing co-ordinator are both trained CEOP ambassadors and will provide yearly E-Safety updates.

Teaching pupils about E-safety is an essential part of the school's e-safety provision. At Highlands Primary School we feel that pupils need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

• Key e-safety messages should be reinforced as part of a planned programme of assemblies

• Pupils should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school

• Rules for use of ICT systems are regularly taught in assemblies and our toy monkey is a symbol to remind children of the safe use of the internet.

• Staff should act as good role models in their use of ICT, the internet and mobile devices

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum. The school's E-Safety Long Term Plan ensures that children are regularly taught about the importance of staying safe whilst online.

• In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use.

• Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the pupils visit.

Staff must ensure that they:

• At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

• Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

• Transfer data using encryption and secure password protected devices.

When using communication technologies the school considers the following as good practice:

• The official school email service may be regarded as safe and secure and is monitored.

• Users need to be aware that email communications are monitored

• Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

See Safeguarding Policy for further details.

Amended January 2018 by Ruth Murray