Language, Learning, Lives

E-Safety Policy Statement

Date of last review: September 2019
Lead reviewer: Nicola Penlington, Laura Cantwell and Mrs K Holmes
Approved by: Local Governing Body
Approved on: Autumn 2019
Date of next review: September 2021

Contents

1. Scope of the Policy

The school believes a clear e- safety policy, consistently and fairly applied, underpins effective education. The school will ensure that all school staff, children and parents should all be clear of the high standards of behaviour expected by all staff at all times. The e-safety advice will be supported and backed-up by the head teacher and the school Leadership team.

What do we mean by E-Safety?

E-Safety is about safe and responsible use of modern technology to include:

- existing and future stationary/mobile electronic devices
- existing and developing Internet-based technologies
- used for the purposes of learning, business and recreation.

Introduction

The school recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use.

Our approach is to implement appropriate safeguards within the school, while supporting staff and children to identify and manage risks independently and with confidence. Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education of children in e-safety is therefore an essential part of the schools' e-safety provision. Children and young people need the help and support of the academy to recognise and avoid e-safety risks and build their resilience. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies.

In furtherance of our duty to safeguard children, we will do all that we can to make our children and staff stay e-safe and to satisfy our wider duty of care. E-safety will be a focus in all areas of the curriculum and staff should take active steps to reinforce e-safety messages across the curriculum.

This E-safety policy should be read alongside other relevant school policies, including Safeguarding, Acceptable Use, Anti Bullying and the Disciplinary procedure.

2. Principles

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

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and

empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside of the school but are linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and confiscation of electronic devices and the deletion of data. In the case of both Acts, action can only be taken over issues covered by the published Behaviour and Rewards Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school. In order to safeguard our community external agencies including the Police may also become involved.

3. Roles and Responsibilities

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

The School Governors

The School Governors are responsible for the overall effectiveness of the policy. This will be carried out by the Governing Body receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has the role of Safeguarding Link, which includes e-safety.

The Head teacher /SLT and Safeguarding Team

The Head teacher has a duty of care for ensuring the safety of members of the school community and therefore has overall responsibility for e-safety in the school.

The Head teacher and the Safeguarding Team have day to day responsibility for e-safety. They share the leading role in establishing, reviewing and implementing the school e-safety procedures, providing training and advice for staff and liaising with outside bodies in relation to e-safety issues.

Children

Children should be aware of the significant risks of exposing themselves or others to personal harm or danger because of inappropriate use of IT and digital media and should manage their use of IT to minimise these risks.

Children are responsible for using the school IT systems and generally understanding the importance of adopting good e-safety practice when using digital technologies in and out of school.

Parents and carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way.

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the school website and information about national and local e-safety campaigns and literature.

There are specific links and guidance to E-Safety for parents and children on the school website, and regular updates sent as reminders and new information.

Staff

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 and have read, understood and signed the staff Acceptable Use Policy (AUP). Staff that work directly with pupils are also responsible for helping them understand the importance of e-safety and how they can reduce exposing themselves to risk.

IT Support

IT Support is responsible for ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack and has all the necessary controls in place, such as web filtering and password protection to reduce the risk of e-safety issues arising. IT Support also monitor staff and pupil usage of the internet.

4. Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying and/or exploitation to take place.

Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is increasingly common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

5. Social Media – Protecting Professional Identity

The Acceptable Usage Guidance for staff/Volunteer and children set out the expectations about the appropriate use of social media by staff, pupils and parents/carers. This guidance must be followed in order to ensure that staff, pupils and

parents/carers do not engage in any activity which may cause them to breach acceptable standards of conduct.

6. Unsuitable or Inappropriate Activities/Responding to Incidents of Misuse

The Acceptable Usage Guidance for staff/Volunteer and children set out the requirements in relation to reporting unsuitable or inappropriate activities. Where such activities also raise a safeguarding concern, the schools Safeguarding Policy, and relevant procedures must be followed.

7. Actions and Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. Incidents will be dealt with as soon as possible in a proportionate manner and members of the school community will be made aware that incidents have been dealt with. Incidents of misuse will be dealt with through normal behaviour and disciplinary procedures.

8. Personal Data

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR) announced in 2016.

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.

The Futures Trust encourages single sign-in across schools and the use of Microsoft Cloud to store and transfer files, with password expectations followed.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected. (many memory sticks / cards and other mobile devices cannot be password protected)
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school / academy policy once it has been transferred or its use is complete.