e-Safety Policy

Introduction

The purpose of this policy is to:

- protect and educate pupils and staff in their use of technology
- have the appropriate mechanisms to intervene and support any incident where appropriate

The breadth of issues classified within e-safety is considerable, but can be categorised into three areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful material
- **contact:** being subjected to harmful online interaction with other users
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm

Expectations

All Education Fellowship schools are expected to:

- have extensive provision for e-safety with all the staff, including members of the wider workforce, sharing responsibility for it. Assemblies, tutorial time, personal, social, health and education lessons, and an age-appropriate curriculum for e-safety all should be used to help pupils to become safe and responsible users of new technologies
- provide 'managed' systems rather than 'locked down' systems in order to provide better knowledge and understanding of how to stay safe. Pupils should be given enough opportunities to learn how to assess and manage risk for themselves
- have senior leaders, governors, staff and families working together to develop a clear strategy for e-safety. Policies will be reviewed regularly in the light of technological and statutory developments
- recognise that they need to keep developing relationships with families to continue to support e-safety at home
- make good use of the views of pupils and their parents to develop their e-safety provision

Requirements for schools

All Education Fellowship schools will:

- audit the training needs of all staff and provide training to improve their knowledge of and expertise in the safe and appropriate use of new technologies
- work closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at school
- use pupils' and families' views to develop e-safety strategies
- manage the transition from locked down systems to more managed systems to help pupils understand how to manage risk; to provide them with richer learning experiences; and to bridge the gap between systems at school and the more open systems outside school
- provide an age-related, comprehensive curriculum for e-safety that enables pupils to become safe and responsible users of new technologies
- work with their partners and other providers to ensure that pupils who receive part of their education away from school are e-safe
- systematically review and develop their e-safety procedures, including training, to ensure that they have a positive impact on pupils' knowledge and understanding

Common risks

Content

- exposure to inappropriate content, including online pornography; ignoring age ratings in games (exposure to violence, often associated with racist language); and substance abuse
- lifestyle websites, for example pro-anorexia, self-harm or suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information

- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

Why is this important?

Technology offers considerable opportunities and is constantly evolving. Access is currently becoming universal and increasingly more mobile, and pupils are using technology at an ever earlier age.

Just because these technologies are online, children are no less susceptible to potential harm compared to the physical world. This makes it vitally important that pupils and staff are fully prepared and supported to use these technologies responsibly.

Key compliance requirements

Whole school consistent approach	All teaching and non-teaching staff can recognise and are aware of e-safety issues. High quality leadership and management make e-safety a priority across all areas of the school (the school may also have achieved a recognised standard, for example the e-Safety Mark). A high priority is given to training in e-safety, extending expertise widely and building internal capacity. The contribution of pupils, parents and the wider school community is valued and integrated.
Robust and integrated reporting routines	School-based reporting routes that are clearly understood and used by the whole school, for example online anonymous reporting systems. Report Abuse buttons, for example CEOP. Clear, signposted and respected routes to key members of staff. Effective use of peer mentoring and support.
Staff	All teaching and non-teaching staff receive regular and up-to-date training. One or more members of staff have a higher level of expertise and clearly defined responsibilities.
Policies	Rigorous e-safety procedures are in place, written in plain English,

And procedures	contributed to by the whole school, updated regularly and ratified by governors. This e-safety policy should be integrated with other relevant policies such as behaviour, safeguarding and anti-bullying. This e-safety policy should be supported by the Acceptable Usage Policy that is understood and respected by pupils, staff and parents.
Education	An age-appropriate e-safety curriculum that is flexible, relevant and engages pupils' interest; that is used to promote e-safety through teaching pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. Positive rewards are used to cultivate positive and responsible use. Peer mentoring programmes.
Infrastructure	Recognised Internet Service Provider (ISP) or Regional Broadband Consortium (RBC) together with age-related filtering that is actively monitored.
Monitoring and Evaluation	Risk assessment taken seriously and used to good effect in promoting e-safety. Using data effectively to assess the impact of e-safety practice and how this informs strategy.
Management of Personal Data	The impact level of personal data is understood and data is managed securely and in accordance with the statutory requirements of the Data Protection Act 1998. Any professional communications that utilise technology between the school and pupils/students, their families or external agencies should: • take place within clear and explicit professional boundaries • be transparent and open to scrutiny • not share any personal information with a child or young person.

Indicators of inadequate practice

- Personal data is often unsecured and/or leaves school site without encryption
- Security of passwords is ineffective, for example passwords are shared or common with all but the youngest children
- Policies/procedures are generic and not updated
- There is no progressive, planned e-safety education across the curriculum, for example there is only an assembly held annually
- There is no internet filtering or monitoring

- There is no evidence of staff training
- Children are not aware of how to report a problem

This policy should be used in conjunction with The Education Fellowship Information Technologies Handbook and other Education Fellowship IT policies including Acceptable Usage, Data Protection, Bring Your Own Device, Copyright, Intellectual Property Rights and Patents and School Technical policies.