

E-Safety Policy.

Continuing The Learning Journey Together

**Date: March 2019**

**Review: March 2020**

Social Media Policy



**Introduction**



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

All members of the Park Hall family contribute to the life of our happy, friendly and successful school. We ensure that our values; honesty, enjoyment, achievement, respect, teamwork are at the heart of all that we do. We are passionate about working in partnership with pupils, parents and carers to protect the Park Hall family.

E-Safety depends on effective practice at a number of levels:

Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.

Sound implementation of E-Safety policy, in both administration and curriculum, including secure network design and use.

Safe and secure broadband; including the effective management of filtering.

National Education Network standards and specifications.

This policy is based on the Department for Education’s statutory safeguarding guidance, [Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2), and its advice for schools on [preventing and tackling bullying](https://www.gov.uk/government/publications/preventing-and-tackling-bullying) and [searching, screening and confiscation](https://www.gov.uk/government/publications/searching-screening-and-confiscation). It also refers to the Department’s guidance on [protecting children from radicalisation](https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty).

It reflects existing legislation, including but not limited to the [Education Act 1996](https://www.legislation.gov.uk/ukpga/1996/56/contents) (as amended), the [Education and Inspections Act 2006](https://www.legislation.gov.uk/ukpga/2006/40/contents) and the [Equality Act 2010](https://www.legislation.gov.uk/ukpga/2010/15/contents). In addition, it reflects the [Education Act 2011](http://www.legislation.gov.uk/ukpga/2011/21/contents/enacted), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils’ electronic devices where they believe there is a ‘good reason’ to do so.

The policy also takes into account the [National Curriculum computing programmes of study](https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study).

**What is E-Safety?**

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

**Aims and Objectives**

* To ensure that all members of our academy community understand and are collectively committed to promoting respectful and responsible internet use.
* To ensure that staff and pupils are aware of the benefits and risks associated with internet use and the use of social media. We actively discourage the use of social media by our pupils.
* To ensure that all necessary measures are in place to safeguard all; *protecting the Park Hall family*.
* To ensure that pupils feel safe and secure and are aware of how to keep themselves safe online.
* To ensure that all members of our Park Hall community are aware of their responsibilities to safeguard themselves and others when accessing the internet and engaging in online activities.

**Reviewing the E-Safety Policy**

The E-Safety Policy relates to other policies including those for Computing, Anti-bullying, Education PREVENT and for Safeguarding. The Computing Leader will also act as E-Safety Leader. The E-Safety Policy and its implementation will be reviewed annually.

**Learning and Teaching**

Why are new technologies and internet use important?

* The Internet is an essential element in 21st century life for education, business and social interaction. The academy has a duty to provide students with quality Internet access as part of their learning experience.
* Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
* The purpose of Internet use in Park Hall Academy is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school’s management information and business administration systems.
* Pupils use the Internet widely outside of Park Hall Academy and will need to learn how to evaluate Internet information and to take responsibility for their own safety and security.

**Internet Use Will Enhance Learning**

* Academy Internet access will be designed expressly for pupil use and will include Internet usage monitoring and web filtering appropriate to the age of pupils.
* Pupils will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use.
* Internet access will be planned to enrich and extend learning activities and to raise attainment and achievement. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
* Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils’ age and maturity.
* Pupils will be educated in the effective use of the Internet in research, including the skills of effective knowledge location, retrieval and evaluation.
* Pupils will be taught how to evaluate Internet content.
* The academy will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
* Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

**Pupils Will be Taught How to Stay E-Safe.**

At Park Hall Academy we are passionate about ensuring that our learners develop sound knowledge, understanding and skills; to enable them to actively demonstrate effective e-safety practices. Curriculum planning will build on pupil’s previous learning and is progressive. Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

At Park Hall Academy, we educate our very youngest learners about the importance of e-safety as we recognise that pupils are accessing an online world both in the home and school environment.

In Key Stage 1, pupils will be taught to:

* + Use technology safely and respectfully, keeping personal information private
  + Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

* + Use technology safely, respectfully and responsibly
  + Recognise acceptable and unacceptable behaviour
  + Identify a range of ways to report concerns about content and contact

The safe use of social media and the internet will also be covered in other subjects where relevant. The academy will use assemblies to raise pupils’ awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

**Cyber-Bullying (see separate anti-bullying policy)**

The rapid development of and widespread access to technology has provided a new medium for ‘virtual bullying’, which can occur in and outside school. Cyber-bullying is a different form of bullying which can happen beyond the school day into home and private space, with a potentially bigger audience, and more accessories as people forward on content.

We teach all Park Hall pupils to ‘tweet other’s as you would like to be tweeted.’ The importance of respectful online communications is explicitly taught and all pupils and parents are aware of our expectations.

**Radicalisation and Extremism**

Park Hall Academy takes an active role in protecting pupils from the risks of extremism and radicalisation. Keeping children safe from risks posed by terrorist exploitation of social media is approached in the same way as safeguarding children from any other online abuse. In the same way teachers are vigilant about signs of possible physical or emotional abuse, we are vigilant about any signs of radicalisation or extremism in any of our pupils. We follow the same safeguarding procedure to ensure all children in our care are well looked after.

For more information on Radicalisation and Extremism please follow the link on our website on the e-safety page.

**Managing Internet Access**

**Information System Security**

Academy ICT systems capacity and security will be reviewed regularly.

Virus protection will be updated regularly.

Academy systems continually remind users that school systems are protected by forensic software. Any irregularities are monitored by the Principal and E-Safety Leader, any breach of the academy policies could result in disciplinary actions.

**E-mail**

*(Currently blocked and only opened if Teacher requests e.g. covering within the curriculum)*

* Pupils may only use approved e-mail accounts/messaging systems on the academy system with express permission and approval from staff.
* Pupils must immediately tell a teacher if they receive offensive e-mail or messages. Pupils must ensure that such emails are not deleted.
* Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

**Publishing Pupils’ Images and Work**

Images, published to the web, that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. Pupils’ full names will not be used anywhere on the Web site, particularly in association with photographs.

Written permission from parents or carers will be obtained before images of pupils or pupils’ work are published on the school Web site. This is obtained on entry to school. No photographs of Looked after Children should be displayed.

**Social Media and Personal Publishing**

The academy will block/filter access to social media sites.

Newsgroups will be blocked unless a specific use is approved.

Pupils and staff will be advised never to give out personal details of any kind which may identify them or their location.

**Managing Filtering**

The academy will work in partnership with the SBMAT, Stoke on Trent Safeguarding board and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Lead. (Miss A James/ Miss Dono who will directly report to SLT and block accordingly).

The Computing Leader will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

**Managing Emerging Technologies**

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the academy is allowed.

Pupils are not allowed mobile phones in school unless specific permission has been given by the Principal or Vice Principal. Academy staff and visitors must ensure that mobile devices are switched off and secured out of view from pupils. We do not use mobile phones to record images of pupils or access/comment on social media during school time.

**Protecting Personal Data**

Personal data is recorded, processed, transferred and made available, according to the Data Protection Act 1998. With effect from May 2018 our academy will comply with the General Data Protection Regulation requirements.

**Password Security**

All devices that have access to a) the internet and b) the academy network must be password protected. The purpose of this is to prevent data loss and protect pupils and staff.

Staff passwords

Staff each have their own username and unique password. Staff generate their own password and understand that they must not share passwords. Records of staff passwords are not stored but the passwords can be overwritten or reset by the network administrator. Staff are expected to change their passwords at least annually to ensure that they remain secure. Staff with access to sensitive data change their passwords every term.

Pupil passwords

Each pupil has their own username and password with the exception of foundation stage. Passwords are generated by the IT Technician and a record of the passwords is stored on the network. Children are taught not to share their passwords with anyone.

Tablet PIN codes

All tablets at Park Hall have a 4 or 6 digit PIN code. There are 3 different PIN codes which all staff should know.

**Policy Decisions**

*Authorising Internet access*

All staff must read and adhere to the academy Acceptable use policy before using any academy ICT resource.

Access to the Internet for pupils, will be by supervised access to specific, approved on-line materials.

All staff, governors and volunteers must read and understand the related computing policies (see related policies).

**Assessing Risks**

The academy will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the academy nor St. Bart’s Academy Trust can accept liability for the material accessed, or any consequences of Internet access. If unsuitable material appears, the E-Safety Leader & Senior Leaders will be informed so that relevant filtering can be completed.

The academy will audit ICT provision to establish if the E-Safety policy is adequate and that its implementation is effective.

**Handling E-Safety Complaints**

Complaints of Internet misuse will be dealt with by the class teacher and where necessary a senior member of staff. Records of incidents will be recorded. Any complaint about staff misuse must be referred to the Principal. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Parents and pupils are expected to work in partnership with the academy to resolve issues or concerns.

Where academy policies are breached, we reserve the right to restrict or remove a pupil’s access to the internet or technologies.

If necessary the academy will liaise with external agencies such as the police or Channel Panel (to refer incidences relating to radicalisation or extremism

**Communicating the E-Safety Policy**

*Introducing the E-Safety policy to pupils*

The child friendly policy is displayed within all classrooms and our computing suite. This is discussed with pupils at the start of each year and regularly referred to throughout the year. Pupils sign and agree to adhere to the academy expectations contained within this policy.

Pupils are informed that network and Internet use will be monitored through the use of forensic software.

**Staff and the E-Safety policy**

***All staff must accept the terms of the academy Acceptable Use policy before using any Internet resources within the academy.***

All staff must adhere to E-Safety Policy.

All staff are informed that all computer and internet use is monitored through forensic software. Discretion and professional conduct is essential.

**Continued Professional Development**

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. In addition, all staff members will revisit or review this training as part of our annual safeguarding updates.

**Enlisting Parents’ Support**

Parents’ attention will be drawn to the academy E-Safety Policy in newsletters, the academy prospectus, on the academy website and through parent workshops.

This policy was reviewed and updated by the Principal, Children’s Safeguarding Board, Computing and E-Safety Leader and Governor with responsibility for Computing & E-safety.