Witton Park Academy

E-LEARNING AND E-SAFETY POLICY

Reviewed June 2018

By Helen Cook

Succeeding Together

wittonpark.org.uk

Succeeding Together

WITTON PARK ACADEMY
E-LEARNING AND E-SAFETY POLICY

What is e learning?

E Learning is the use of technology to support teaching, learning and management at Witton Park Academy Business & Enterprise College.

Our Vision

Every member of the school community becomes **e confident** as part of the Blackburn with Darwen vision for "schools for the future" and Lifelong Learning.

For teachers and support staff e confidence incorporates using technology for teaching (e.g. presentation of ideas), for learning (e.g. using an ICT suite with a class) and for management (e.g. analysing exam results using a spreadsheet). Whilst for students e confidence incorporates good practice, working safely, understanding when and how to use technology appropriately.

The whole school strategy at Witton Park Academy Business & Enterprise College comprises of

1. Adherence to a whole school E-Safety Policy.
2. Supporting the use of ICT including the dissemination of good practice and the development of on-line environments.
3. Increasing the use of ICT to promote inclusion through the use of lap tops, the VLE and other hardware.
4. Ensuring that every member of staff has access to ICT facilities and e mail.
5. Continuing professional development with coherent personal learning development, support and access – for all leaders, teaching and non-teaching staff to ensure that ICT contributes to the effectiveness of lifelong learning strategies

Teaching and Learning

As the children's access and understanding expands, so should the guidance and rules to ensure safe access use of the internet.

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school 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 took for staff and pupils.

Pupils will be taught how to evaluate Internet content appropriate to their age.

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught about responsible Internet use and given clear objectives for its use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation appropriate to their age group.
- Sanctions for inappropriate use of the internet will be explained to the children.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is updated regularly.
- Security strategies will be discussed with Blackburn with Darwen.

Managing filtering

- The school will work with the LA, DofE 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-Learning Manager and the LA will be informed so that they can take appropriate action.
- Staff can request re-categorisation of Internet sites, which will be approved by the E-Learning Manager.

Staying Safe

The school will ensure that pupils and parents are aware of e safety issues. A list of useful addresses and resources is included in this document.

- The school internet access is designed expressly for pupil use and includes appropriate filtering.
- Users may only use approved digital methods of communication on the school system eg: not forwarding chain letters, no cyber-bullying.
- Pupils will be taught to tell an adult immediately about any offensive communications they receive or any inappropriate content they may encounter using digital technology.
- Pupils and staff will use equipment responsibly.
- Pupils will be advised never to give out personal details of any kind why may identify them or their location or arrange to meet anyone without specific permission.
- Pupils and parents will be advised that the unsupervised use of social network spaces outside school is inappropriate for pupils.
- Staff are also advised that the use of social networking websites may compromise their professional standing with pupils, parents and colleagues. The school therefore recommends staff not to use these websites.

Published content

Any information that can be publicly accessed should be classed as published whether in electronic or paper format.

- Electronic communication sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- General contact details should be the school address, email and telephone number. Staff or pupils' personal information will not be published
- The headteacher, or the E-Learning Manager, will take overall editorial responsibility for the public website and ensure that content is accurate and appropriate. The Headteacher's PA will update the website content on behalf of the school.

Publishing pupil's images and work

- Staff and pupils using digital cameras, video recorders or sound recorders will ensure that they inform others before recording them and always use equipment in a respectful manner.

- Photographs that include pupils will be selected carefully and will not enable pupils to be individually identified.
- Pupils full names will not be used anywhere, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs or videos of pupils are published.
- Where pupils work is published the school will ensure that the child's identity is protected.

Managing emerging technologies

- The educational benefit of emerging technologies and any potential risks will be considered before it is used in school.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Personal pupil data and pictures should not be removed from the school (eg: on laptops, USB memory sticks) in order to prevent accidental loss. More specific guidance is given in the Data Protection Policy.

Policy Decisions

Authorising Computer access

- All users must read and sign the Acceptable Computer Use Statement, shown in Annex A, before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up to date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Parents will be asked to sign and return a consent form for use of the school network and VLE. The VLE agreement is shown in Annex B.

Assessing risks

- The school 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 school nor Blackburn with Darwen LEA can accept liability for the material accessed, or any consequences of Internet access. Any inappropriate access whether intentional or unintentional will be reported to the E-Learning Manager and to the LA where necessary.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Use of Resources

- Only authorised software will be used, in accordance with the license agreement.
- Users will be held responsible for any unauthorised software which is found on their network areas, or on devices issued to them by school.
- Users are expected to manage their own file areas, within the quota's and restrictions imposed by the school.
- Suspected misuse of IT resources will be investigated, and may result in sanctions being imposed on the user.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff and where appropriate inform the LA and IT Team.
- Any complaint about staff misuse must be referred to the headteacher.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure on request.

Communications Policy

Monitoring

- The school may, at its discretion, monitor and record any logon, attempted logon, network traffic, files created and Internet sites visited.
- The school reserves the right to delete any file from the school network. Eg inappropriate naming or content.
- The school reserves the right to delete any file on a portable device attached to any school computer, irrespective of the owner of the portable device, in order to protect the integrity of the system.
- Any log files created may be reviewed at a later date, and may be made available to external agencies, to ensure compliance with school policies and UK legislation

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and internet use will be monitored and traced to the individual device or login.

Staff and the e-safety policy

- All staff will be given the school's e-safety policy and its importance explained.
- Staff should be aware that internet traffic may be monitored and traced to individual device or login. Discretion and professional conduct is essential
- The school may use monitoring software where this is available to ensure that inappropriate materials are not being stored or used on school equipment.

Reviewed by Helen Cook
June 2018

Date of next review: June 2019