LARKS HILL

JUNIOR & INFANT

SCHOOL

E-Safety Policy

The Acceptable Use of the Internet and related Technologies

Our e-Safety Policy has been written by the school, building on the London Grid for Learning (LGfL) exemplar policy and Becta guidance. It has been agreed by the senior management and approved by Governors. It will be reviewed annually.

Written by : Ms S. Atkinson
Reviewed : Spring Term 2014

Pontefract Academies Trust

Pontefract Education Trust

Larks Hill J & I School
E-Safety Policy

1. Context

Harnessing Technology: Transforming learning and children's services (http://www.dfes.gov.uk/publications/e-strategy/) sets out the government plans for taking a strategic approach to the future development of ICT.

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005

The Green Paper Every Child Matters (See The Children Act 2004 http://www.opsi.gov.uk/acts/acts2004/20040031.htm) and the provisions of the Children Act 2004 (See Every Child Matters website [http://www.everychildmatters.gov.uk]), Working Together to Safeguard Children sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and

the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

2. The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- Snapchat and screen grabs
- e-mail
- texting/sexting/cyberbullying
- phishing emails and websites
- clickjacking (trying to get people to click on malware or other links)
- Instant messaging (http://www.msn.com, http://info.aol.co.uk/aim/) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.myspace.com / www.piczo.com / www.bebo.com / www.facebook.com / http://www.hi5.com)
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites and online gaming with chat facilities such as X-Box 360 or DSI (Popular online gaming sites: www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/)
- Music download sites (Popular http://www.apple.com/itunes/ http://www.napster.co.uk/ http://www-kazzaa.com/, http://www-livewire.com/)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications.
- Online loans (for older school children)

3. Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-Safety education programme for pupils, staff and parents.

4. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The headteacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to a member of the senior management team.

- Our school **E-Safety Co-ordinator** is Sally Atkinson

Governors:

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving relevant information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety

The role of the E-Safety Governor will include:

- updates when necessary with the E-Safety Governer
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Esafety Coordinator.
- The Headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The Senior Leadership Team will receive updates when necessary from the E-Safety Co-ordinator
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff

Esafety Coordinator

- leads on safety
- writes the Esafety Policy
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority

- liaises with school ICT technical staff
- receives reports of e-safety incidents and organises for a log of incidents kept in the office to inform future e-safety developments
- attends relevant meeting / committee of Governors
- updates when necessary to Senior Leadership Team

Designated person for child protection / Child Protection Officer
A person should be trained in e-safety issues and be 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

Network Manager / Technical staff:
The ICT Co-ordinator and Alamo ICT Technician are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the school's networks through a properly enforced password protection policy
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE / email is monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator /Headteacher
- Filtering requests for blacklisting or whitelisting are authorised by the ICT Coordinator/Headteacher before reporting to the Local Authority/ PAT/PET blocking system administrator.

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 / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator/Headteacher / ICT Co-ordinator for investigation / action / sanction
- digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- students / pupils understand and follow the school e-safety and acceptable use policy
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons and any 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 as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Students / pupils:

- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- 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, if related cto their membership of the school

Parents / Carers

- Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:
- endorsing (by signature) the Student / Pupil Acceptable Use Policy
- accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

5. Safeguards in Place

The schools broadband provider InTechnology provide a Becta accredited filtering system good fire wall which blocks many sites or searches that are inappropriate for Primary children including social network sites, dangerous, sexually explicit or gaming sites.

However, even with these measures in place, inappropriate sites can still very occasionally be accessed. If a site is found that needs blocking, the school can report this to the schools IT support manager (Alamo) and it can be blocked from further access.

Safety posters are displayed in the ICT suite as well as children having E-safety reminders at the beginning of each school year.

Each pupil has a personal log-in and staff members also have a password which they should keep secret. Our ICT maintenance contractor (Alamo) is the only person to have access to change software/programming/log-in information. Some children also have access to SAM Learning (revision tool) at school and from home. For this they have a personal, secure log-in. Details of their use of SAM learning is tracked and accessed by school and SAM Learning.

The school has a website (www.larkshill.wakefield.sch.uk) maintained by our admin team and developed / hosted by Essentia Design. The website provides a communication link to parents and carers as well as displaying information about the school, photographs and news items. Care is taken on the school website not to publish any personal information about staff or pupils.

All parents are asked to notify school in writing if they do not give consent for images to be published in the local media / web site.

6. How will complaints regarding E-safety be handled?

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. It is made clear to staff and taught to pupils how to handle situations of this nature when they occur.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview / counselling by the Learning Mentor / e-Safety Coordinator (Headteacher);
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system];
- referral to LA / Police.

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

7. Out of school issues

The school can offer help and inform parents/carers if issues out of school are affecting pupils during their time at school, but cannot sanction event or actions that happen out of school.

This policy should be read with reference to the following policies:

- Data protection policy.
- Child Protection /Safeguarding Policy
- Social Media Policy

8. Final Comments

This policy is by no means meant to discourage the use of the internet in school for educational work and in free time (e.g. in golden time/breakfast club). However, care must be taken to make children and staff aware of the safety measures they should take when using computers so they become responsible users themselves.

ICT technology is one of the most progressive and useful inventions of our time and we should embrace it into our lives.

Further Guidance:

Larks Hill Staff Guidance

Staff Training