PARKSIDE
COMMUNITY SCHOOL

Parkside Community School On-line Safety Policy

Date of Policy: November 2011
Member of Staff Responsible: Mr Steve Stringer, Head of Faculty: Vocational
Review Date: November 2017

Approved by SLT on 20 October 2016
Approved by Jean Horton, Chair of Governors on 20 October 2016
Approved by Governors Health & Safety Committee on 14 November 2016 (Min No:14/2016/17.14)
Minutes of the meeting approved by Full Governors on 12 December 2016

'This policy has been impact assessed in the light of all other school policies including the Disability Equality Scheme.'

Please note the term Subject Leaders relates to Faculty Leaders, Core Leaders and Lead Teachers at Parkside School.

Parkside Community School believes that the use of Information and Communication Technologies (ICT) brings great benefits. Recognising the safeguarding issues that form the structure of this policy will help to ensure appropriate, effective and safer use of ICT fixed and mobile technologies by Parkside students.

The On-Line safety Policy complements the following Parkside policies:

- ICT Policy
- Computer Usage, Internet Access and Electronic Mail
- Rewards and Sanctions Policy
- Anti-Bullying Policy
- Personal, Social and Health and Economic Education Policy

1. Policy author, contributors and review protocol

1.1 Policy author

- Mr Steve Stringer, Head of Faculty: Vocational

1.2 Policy contributors

- Mr J E Crawley: Network Manager – On-Line-Safety Co-ordinator Technical.
- Mrs R Hammond: Deputy Headteacher: Teaching & Learning
- Mr G Dearman: Designated Safeguarding Lead
- The policy has been written in compliance with the guidance from the Department For Education (DFE), Specialist Schools and Academies Trust (SSAT) and Derbyshire, Sheffield and Kent Local Authorities.

1.3 Review protocol

- The policy will be reviewed by the Strategic ICT Development Group (SDG) at the first meeting of the academic year. Any modifications to the policy will be approved by the Governing Body.

2. Managing information systems

2.1 Information system security

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by a virus check.
- Unapproved software will not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The Network Manager will review system capacity regularly.

2.1.1 Local Area Network (LAN) security protocol

- Users must act reasonably. An example of an unreasonable act would be the downloading of large files during the working day which would affect the service that others receive.
- Users must take responsibility for their network use.
- Workstations will be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.

- Virus protection for the whole network must be installed and current.
- Access by wireless devices will be pro-actively managed.

2.2 Wide Area Network (WAN) security protocol

- All Internet connections must be arranged via the School, East Midlands Broadband Consortium and Derbyshire County Council (DCC) to ensure compliance with the security policy.
- Decisions on WAN security are made on a partnership basis between the School and DCC.

2.2. Managing email access

- Students will only use an approved email account created by the Network Manager. The structure of a school email address is username@parkside.derbyshire.sch.uk
- Students must immediately inform a teacher or the Network Manager if they receive offensive email.
- Students must not reveal personal details of themselves or others in an email communication, or arrange to meet anyone without specific permission from an adult.
- Access in school to external personal email is blocked.
- Email sent to external organisations will be written carefully and approved by a teacher before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain messages is not permitted.
- Staff should only use school email accounts to communicate with students as approved by the SDG.
- Staff will not use personal email accounts during school hours or for school related purposes.

2.3 Published content management

2.3.1 Management of the publishing vehicles

The vehicles employed for publishing content are the school website, Parkside Learning Platform (PLP) and termly digital newsletters and their content must adhere to the following:

- The contact details published should be the school address, email and telephone number. Staff and student personal information must not be published.
- Email addresses will be published carefully, to avoid being harvested for spam.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the School’s guidelines for publications including respect for intellectual property rights and copyright.

2.3.2 Publishing student images and work

- Images that include students and staff will be selected carefully and will not provide material that could be reused.
- Full names of students and staff will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of students are electronically published.
- Students' work can only be published with their permission or that of their parents.

2.4 Managing social networking and social media

- The School will control access to social media and social networking sites.
- Students receive discrete lessons and assemblies informing them:

    - never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, instant messaging and email addresses, full names of friends/family, specific interests and clubs.
    - not to place personal photos on any social network space. Students will understand how public the information is and consider using private areas. Advice will be given regarding background detail in a photograph which could identify the student or his/her location.
    - on the importance of security and to set passwords; deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others by making profiles private.
    - not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

- Staff official blogs or wikis will be password protected and run from the school website with approval from the Strategy Development Group (SDG). Staff are advised not to run social network spaces for pupil use on a personal basis.
- If personal publishing is to be used with students then it must use age appropriate sites suitable for educational purposes. Personal information must not be published and the site should be moderated by the Network Manager.

2.5 Managing internet filtering

- The school will work with Derbyshire County Council and East Midlands Broadband Consortium to ensure that systems to protect students are monitored, reviewed and improved.
- If staff or students discover unsuitable sites, the URL must be reported to the Network Manager.
- The school's broadband access will include filtering appropriate to the age and maturity of students.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported to appropriate agencies such as Internet Watch Foundation (IWF) or Child Exploitation and Online Protection Centre (CEOP).

2.6 Managing video conferencing

The equipment and network

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses should not be made available to other sites.
- Videoconferencing contact information should not be put on the School website.
- The equipment must be secure and if necessary locked away when not in use.
- School videoconferencing equipment should not be taken off school premises without permission.

The user

- Students should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing should be supervised appropriately for the students' age.
- Parents and carers should agree for their children to take part in videoconferences, as part of the annual return.
- Only the Network Manager will be given access to videoconferencing administration area or remote control pages.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of the videoconference should be clear to all parties at the start. Recorded material will be stored securely.
- If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Dialogue with other conference participants must be established before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material that is appropriate for the class.

2.7 Managing emerging technologies

- Emerging technologies will be examined by the SDG for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons unless to support teaching and learning. The sending of abusive or inappropriate text, picture or video messages is forbidden.

2.8 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

3. Internet management

3.1 Internet access

- The School will maintain a current record of all staff and students who are granted access to the School's electronic communications.
- All staff must read and sign the Policy on Computer Usage, Internet Access and Electronic Mail before using any school ICT resource.
- Students must apply for Internet access individually by agreeing to comply with the On-Line Safety Rules.
- Parents will be asked to sign and return a consent form for student access.
- Parents will be informed that students will be provided with supervised Internet access.

3.2 Risk assessment

- The School will audit ICT use to establish if the On-Line Safety policy is adequate and that the implementation of the On-Line Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly by the SDG.

3.2 Internet across the community

- The School will liaise with local organisations to establish a common approach to On-Line Safety.
- The School will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

4. Handling On-Line-safety complaints

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure Policy.
- Any complaint about staff misuse must be referred to the Headteacher.
- All On-Line Safety complaints, incidents and actions taken will be recorded by the School.
- Students and parents will be informed of the complaints procedure via the school website.
- Parents/carers and students will work in partnership with staff to resolve issues.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and Children's Safeguards Unit to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the School's disciplinary and child protection procedures.

5. Cyberbullying

Cyberbullying can be defined as “The use of Information Communication Technologies, particularly mobile phones and the internet to deliberately hurt or upset someone” DCSF 2007.

- Cyberbullying, along with all forms of bullying, will not be tolerated in school. Full details are set out in the Anti-Bullying Policy.
- All incidents of cyberbullying reported to the school will be recorded.
- **There will be clear procedures in place to investigate incidents or allegations of Cyberbullying:**
  - Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.
  - The School will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- **Sanctions for those involved in Cyberbullying include:**
  - The bully will be asked to remove any material deemed to be inappropriate or offensive.
  - A service provider may be contacted to remove content.
  - Internet access may be suspended by the Network Manager for the user for a period of time.
  - Parent/carers may be informed.
  - The Police will be contacted if a criminal offence is suspected.

6. Managing the Parkside Learning Platform (PLP)

- The SDG will monitor the usage of the PLP by students and staff regularly in all areas, in particular message and communication tools and publishing facilities.
- Students/staff will be advised on acceptable conduct and use when using the learning platform.
- Only current student, parent/carers and staff stakeholders will have access to the PLP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the PLP.
- When stakeholders leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns with content may be recorded and dealt with in the following ways:

  a) The user will be asked to remove any material deemed to be inappropriate or offensive.

  b) The material will be removed by the site administrator if the user does not comply.

  c) Access to the PLP for the user may be suspended.

d) The user will need to discuss the issues with a member of the School's Senior
Leadership Team before reinstatement.
e) Parents/carers may be informed.

- A visitor may be invited onto the PLP by a member of the SDG. In this instance there may be an agreed focus or a limited time slot.

7. Communication policy

- All users will be informed that network and Internet use will be monitored.
- An On-Line Safety Scheme of Work (SOW) is in place to raise the awareness and importance of safe and responsible internet use.
- All students new to the School will receive instructions on the responsible and safe use before they are given Internet access.
- A cross-curricular On-Line Safety module will be included in KS3 and KS4 Personal Development covering both safe school and home use.
- On-Line Safety awareness will be part of the ICT SOW transition programme across the Key Stages. Safe and responsible use of the Internet and technology will be reinforced across the curriculum. Particular attention will be given where students are considered to be vulnerable.
- On-Line Safety marketing posters will be visible in all ICT suites.
- All students will participate in an annual On Line Safety lesson.
- All students will receive annual On Line Safety College Assembly.

7.2 Communicating the policy to staff

- The On Line Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the School will implement Acceptable Use Policies.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by the SDG and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use both professionally and personally will be provided.

7.3 Communicating the policy to parents/carers

- Parents'/carers' attention will be drawn to the School's On-Line Safety Policy in the termly newsletter, school prospectus, school website and PLP.
- A partnership approach with parents is the aim. Parkside will explore the capacity to run annual parents' evenings with demonstrations and suggestions for safe home Internet use.
- The On-Line Safety Policy may also be highlighted at other attended events such as Academic Reviews and Sports Day.
- Parents will be requested to sign an On-Line Safety/Internet agreement as part of the Home School Agreement.
- Information and guidance for parents on On-Line Safety will be made available in a variety of formats including an annual On-Line e-Safety letter.

- Interested parents will be referred to organisations listed on the school website.