Pudsey
Grangefield
School

Online Safety Policy

This policy has been agreed by the Governing Body of Pudsey Grangefield School.

Signed …………………………….……..
Chair of Governors

Date approved …………………………………

Date to be reviewed: November 2017

Further information on keeping children safe online, please see the links below:

http://www.leedslscb.org.uk/Practitioners/Support-our-campaigns/Think-before-you-send

Pudsey Grangefield School

Online Policy 2016/17

Policy Statement

New technologies are embedded in everything we do in and outside school. The internet and other communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. The online policy explains how as a school we will help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Purpose

The purpose of this policy is to make sure that the school and staff meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school.

Development / Monitoring / Review of this Policy

The online policy has been written using the e-safety guide for Leeds 2015, e-safety Strategy for Leeds 2015 (both from the Leeds Safeguarding Children Board) and the South West Grid for Learning Guidance. It has been agreed by the Leadership Group and approved by the Governors. All staff have received a copy of the policy.

The online policy was been reviewed and updated every year.

The school will monitor the impact of the policy using:

- Internal logs of reported incidents (from ‘Smoothwall’ web filtering software and SIMS Lesson Monitor)
- Surveys / questionnaires of students, parents / carers ,staff
- Computers are monitored through ‘Future Digital’. This allows the designated staff to monitor resources that are accessed online by students. This monitoring has been put in place from November 2016.

Scope of the Policy

The policy applies to all uses (eg students, staff, Governors, visitors) of the School community who have access to and are users of School’s ICT systems, both in and out of school.

Roles and Responsibilities

Governors:

The ‘Curriculum’ Governor’s sub committee will receive information about how online safety is taught in the curriculum. The ‘Student Support’ Governor’s sub committee will receive information about incidents and monitoring reports.

Principal and Senior Leaders:

- the Principal is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Assistant Principal and the Deputy Principal.
- the Leadership Team will receive online safety updates from the Assistant Principal and Deputy Principal.
- the Principal and Deputy Principal are aware of the procedures to be followed in the event of a serious online safety allegation made against a student or member of staff.

Assistant Principal (online safety)

- is responsible for ensuring that the online safety curriculum is delivered.
- is responsible for ensuring that the ICT infrastructure and procedures are in place.
- liaises with the Deputy Principal to look at online safety incidents to inform future developments.
- reports to the Leadership Team and Governors

Deputy Principal (Student Effectiveness and Relationships)

- is responsible for ensuring that online safety is an integral part of safeguarding policies and procedures in school.
- reports to the Leadership Team and Governors

PGS Network Manager

The Network Manager is 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 network using individual passwords
- that 'Smoothwall' web filtering software is installed, updated and working on the network
- that requests from staff to 'unblock' any educational websites that 'Smoothwall' may block by default are recorded including the URL, name of requester and date it was unblocked. SLT have access to this information
- that 'Future Digital' monitoring software is installed, updated and working on the network
- liaises with RM broadband so that there is suitable external filtering of the internet at source
- liaises with school leadership so that network and internet passwords are given to users
- that any leased iPads are configured to connect to the school filtered internet
- that if any student wants to use their own mobile device to connect to the school wifi, the network manager will register the device and configure it so that it connects to the school's filtered internet. Students will sign the 'Acceptable use policy'.

The Network Manager will also monitor the network to identify any unsuitable downloaded or uploaded material.

RM broadband (internet service provider)

Is responsible for ensuring that there is suitable external filtering of the internet at source.

Teaching and Support Staff:

- should have an up to date awareness of online safety matters and of the current school policy
- should have read, understood the school Code of Conduct for all staff which makes reference to online safety
- use the school email system to communicate with students
- ensure that students understand and follow the 'Responsible and Safe Computer/Online Use' and 'Mobile phones and mobile technologies' policy in the Student Planner.
- monitor ICT activity in lessons, extra curricular and extended school activities, and deal with any misuse in line with the behaviour policy.
- ensure that students understand and follow the 'Mobile phone and mobile technologies' policy in the Student Guide and deal with any misuse in line with the 'Behaviour Policy'
- use SIMS Lesson Monitor to record online incidents
- report any more serious misuse to the Deputy Principal for investigation

Child Protection/Designated Teachers

should be trained in online 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
- Monitor the use of online resources through Future Digital and follow-up any cause for concerns.

Students:

- are responsible for using the school ICT systems in accordance with the 'Responsible and Safe Computer/Online Use' in the Student Planner which they are be expected to sign before being given access to school systems
- must tick to accept the 'Acceptable use policy' when they log on to the school network and therefore the internet.

- must sign the ‘Acceptable use policy’ if they bring their own mobile device into school and want to use the school wifi to connect to the internet.
- know and understand the school policy on the use of ‘Mobile phones and mobile technologies’ as outlined in the Student Planner
- know and understand the school policy on bullying as outlines in the 'Being happy at school' as outlined in the Student Planner and understand how it applies to cyberbullying
- should understand the importance of adopting good online safety practice when using the internet/mobile devises out of school and realise that the school’s Online Policy covers their actions out of school, if related to their membership of the school
- 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. The ‘Think-you-know’ website link will be an icon on RMUnify, the school website contains the ‘click CEOP’ button to give students online access to advice, help and to report abuse.

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 help parents and carers to understand these issues through an Online Safety link on the Pudsey Grangefield School website, and through a planned Online Safety information evening. Parents and carers will be responsible for signing their child’s Student Planner to confirm their support for the ‘Responsible and Safe Computer/Online Use’.

Guests users:

Guests (eg Trainee Teachers, Community Access, Conference Staff) who require access to the school ICT systems and internet will be expected to agree to the ‘Acceptable Use Policy’ before being provided with access to school systems.

Policy Statements

Education – Students

The Assistant Principal will initiate discussions with the Leadership Group to secure adequate and appropriate curriculum provision for online safety for all students.

Online safety education will be provided in the following ways:

- a planned online safety programme will be provided as part of the ICT, tutor time and PSHE curriculum.
- key messages will be reinforced as part of the planned programme of Learning Coach sessions
- at the start of each year form tutors will use the Student Planner to discuss with students the need for them to adopt safe and responsible use of ICT, the internet and mobile devices both in and outside school
- students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- staff should act as good role models in their use of ICT, the internet and mobile devices
- students will be taught in lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- students will take part in European Safer Internet Day each year.
- students will be made aware of the ‘Think-you-know’ website link on RMunify and the ‘click CEOP’ button on the school website for online advice, help and to report abuse.

The school’s Online Safety Policy will be available for students and parents/carers on the school website.

Education – Parents and Carers

The school will seek to provide information and awareness to parents and carers through:

- online safety guidance on the school website
- parent/carer online safety twilight session.

Training

Training – Staff

Training will be offered as follows:

- all staff will receive online safety training as part of Child Protection/Safeguarding training.
- all new staff will receive online safety training as part of their induction programme which will include the school 'Online Policy' and the 'Code of conduct for all staff'.

Training – Governors

Governors will become more aware of online safety as part of their Child Protection and Safeguarding awareness training.

Technical Responsibilites

Infrastructure and equipment-PGS Network Manager
The Network Manager is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible. The school infrastructure and individual workstations are protected by up to date virus software. The network does not contain unsuitable downloaded or uploaded material as is reasonably possible.

Monitoring- PGS Network Manager

The PGS Network Manager is responsible for monitoring user activity on the school network and providing the SLT with reports using the 'Smoothwall' internet filtering software.

Curriculum

Online safety is a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use.
- Where students are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites students visit.
- Students will be taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images

- Parents/Carers will be asked to sign a letter for use of student photographs to allow/not allow the school to use their child's photograph in school publications (eg newsletter, PGS website etc.)
- Staff are allowed to take digital / video images to support educational aims.

Data Protection

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

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data (eg SIMS, excel spreadsheets) minimising the risk of its loss or misuse
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session.

Communications

- The 'Mobile Phone and mobile technologies' policy in the Student Planner states that 'Mobile phones/devices and headphones should be turned off and out of sight (except in social times). Equipment will be confiscated and Parents/Carers will need to come into school to collect the item(s)'

- Students are allowed to use their mobile phones in their social time during breaks and lunch time to make and receive calls and to listen to music. They are expected to use their phones appropriately, they should not use them to access websites which would be blocked by the school.
- Incidents of mobile phone and mobile technology misuse should be recorded on SIMS
- Staff should only use the school email system to send email messages to students or parents/carers.

Unsuitable / inappropriate activities

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to any other information which may be illegal or offensive to staff and students or breaches the integrity of the ethos of the school or brings the school into disrepute. Staff should refer to the 'Code of Conduct for all staff'.

Illegal misuse

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The Deputy Principal should be consulted so that the appropriate procedures can be followed, in particular the reporting the incident to the police and the preservation of evidence.

Incidents of misuse

It is more likely that the school will deal with incidents that involve inappropriate rather than illegal misuse.

Any incidents of misuse by students should be dealt with in line with the ‘Behaviour Policy' and recorded on SIMS Lesson Monitor.

Useful Internet Safety Links

www.ceop.gov.uk - Child Exploitation and Online Protection (CEOP) Centre combines police powers with the expertise of business sectors, government, specialist charities and other interested organisations - all focused on tackling child sex abuse.

www.childnet-int.org - Childnet International a non-profit organisation working with others to help make the Internet a great and safe place for children.

www.chatdanger.com - Childnet’s Chat Danger website gives details about the potential dangers of interactive services like chat, IM, online games, e-mail and mobiles

www.kidsmart.org.uk - Kidsmart is practical internet safety programme website for schools, young people, parents, and agencies, produced by the children's internet charity Child net International. There are lesson plans and accompanying resources to help teach KS2 & 3 students about Internet safety.

www.thinkuknow.co.uk - Think U Know is a site with areas for children and young people aged 5 - 7, 8 - 11, and 11 - 16 as well as for parents, carers and professionals. There is information and guidance as well as some games demonstrating chat room use.

http://www.digizen.org/ Digizen is all about recognizing and dealing with online hazards, and about building safe places and communities and learning how to manage personal information. The site also has links to cyberbullying, social networking.

The school’s Online Policy will be available for students and parents/carers on the school website.