Internet/Online Safety Policy

Park Community Academy

Reviewed September 2023

CONTENTS

Park Community Academy

Internet Policy

This Policy reflects the School's Aims and Objectives in relation to the teaching and learning of Computing. Computing is a foundation subject within the National Curriculum. In the Foundation Stage it is incorporated within Knowledge and Understanding of the World.

1. Why is Internet Access Important?

- The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance PCA's management information and business administration system.

- Access to the Internet is a necessary tool for staff and pupils. It is an entitlement for pupils who show a responsible and mature approach.

2. What are the benefits to PCA?

A number of studies and government projects have indicated the benefits to be gained through the appropriate use of the Internet in education.

These benefits include:

- Access to world-wide educational resources including museums and art galleries:
- Inclusion in current government initiatives;
- Information and cultural exchanges between pupils world-wide;
- Cultural, social and leisure use in libraries, youth clubs and at home;
- Discussion with experts in many fields for pupils and staff;
- Staff professional development – access to educational materials and good curriculum practice;
- Communication with the advisory and support services, professional associations, colleagues and parents and carers;
- Improved access to technical support including remote management of network;
- Exchange of curriculum and administration data with the LEA and DfES.

3. Internet use and Education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's safeguarding provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The Online Safety curriculum should be broad,

relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned and appropriate, Online safety curriculum should be provided as part of Computing, PHSE and should be regularly re-visited and reinforced.
- Key Online safety messages should be reinforced as part of an annually planned activity day, as well as whenever the opportunity arises throughout any other lessons. Online safety is also made a priority at the start of each term, with a focused age appropriate lesson delivered in computing lessons across the key stages
- Pupil's should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information
- Pupil's should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupil's should be helped to understand the need for the pupil Acceptable Use Agreement and be encouraged to adopt safe and responsible use both within and outside of school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices - including wearable devices
- In lessons where internet use is pre-planned, it is best practice that 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
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- Internet access is filtered using FortiGuard and is managed by Blackpool Borough Council (BBC)
- Unsuitable websites are usually blocked by BBC. However, close staff supervision must be in place at all times and particularly during less structured times.
- Regular checks of filtering and monitoring procedures will take place (Monthly) and results shared with SLT, Subject leads and Blackpool Council.

4. Internet Use and Parent/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviour. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, website advice
- High profile events / campaigns eg Safer Internet Day
- Coffee mornings with a focus on online safety
- PCA subscribes to the National Online Safety group who provide training in online safety for parents/carers. Information about this course is regularly sent to families.

5. How will Email be Managed?

- All staff have a personal email address and internal communication is sent through the e-mail system.
- All emails are auto-generated by Blackpool Council and monitored and filtered by them.
- Our IT technician sets the passwords and can change them if needed.
- E-mail should only be used in school for education purposes.
- Pupils should not be allowed to access personal email from the school system
- Pupils may send email as part of a planned lesson
- Pupils are discouraged from sending emails to the staff personal email address and they should be encouraged to use the class email address as a way to contact the staff.
- Incoming e-mail to the school e-mail address will be regarded as public
- Messages sent from school should be regarded in the same way as messages written on school headed paper or via the telephone.
- The forwarding of chain letters will be banned, as will the use of chat lines and social networking sites (e.g Instagram, Facebook, with the exception of Twitter to promote activities within school).
- Internet Safety lessons about the appropriate usage of the internet/email at school/home and wider community.

6. How will Publishing on the Web be Managed?

Our school website is constantly being updated. It is hoped that the site will inspire pupils to work to a high standard, for a wide audience. The aim of the web site is that our children's work is celebrated, to promote the school and publish projects being undertaken. Ground rules are important to ensure that the web site reflects the school's ethos, and the information is accurate and well presented, as well as providing parents, carers and the wider community with information about our school such as, detail about what is on the website.
The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- During school performances such as the Christmas or summer show parents and carers are asked not to take photographs or films of the pupils. At a later date the school will share images or films of students whose own parents or carers have given permission for this. The school makes it clear that this is for personal use and asks that none of this is shared on social media.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment if possible, personal equipment of staff should only be used if no other equipment is available at that time.

These photographs should be transferred to school equipment and deleted as soon as possible. This follows the guidance set out in the school's Mobile Phone Policy.

- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. Staff will not use photographs of any Child Looked After, unless permission has been granted by their carer/Social Services. All pupils' parents/carers must sign a letter of permission regarding their child at the beginning of each academic year.
- Pupils' full names will not be used anywhere on Twitter, Facebook, website, blog, particularly in association with photographs
- Students' work can only be published with the permission of the student/pupil and parents/carers

As the web site can be accessed by anyone on the Internet, the security of staff and pupils needs to be considered carefully.

- The ICT Technician/designated Office Staff will take responsibility to ensure that content is accurate and quality of presentation is maintained.
- It is the Teacher's responsibility to provide the ICT Technician/ designated Office Staff with pictures/pupils work to update the website.
- The point of contact on the web site will be the school address, telephone number and there is also an enquiry form which is monitored by the office staff. Home information or individual email identities will not be published.
- Full names of pupils will not be used anywhere on the web site.

7. What other Internet Applications are available?

The Internet is the underlying technology, i.e. the wires and switches. New applications are being developed to use this ability to communicate, such as chat, newsgroups, iCloud and Web cams as well as through portable hardware such as iPads. Many of these facilities have great potential for education, for instance pupils exchanging live text, speech or video with a similar class in other parts of the UK or abroad, at a low cost. However, the implications for the needs of young users need to be considered, particularly the area of security.

- Pupils will not be allowed to access public chat rooms/social networking sites.
- Newsgroups will only be available to staff.
- New facilities will be thoroughly tested before pupils are given access.

8. How will Internet Access be Authorised?

Access to the Internet will be allocated on the basis of educational need. Children are only allowed to use the Internet in school after asking a teacher.

- Internet access is a necessary part of the statutory curriculum. It is an entitlement for pupils based on responsible use.

- Internet access will be granted to a whole class as part of a scheme of work after suitable instruction on responsible Internet use and after SMART rules have been read and signed by both staff and pupils. (Displayed in each class base)
- Parents have been informed that pupils are provided with supervised internet access (annual letter sent home, appendix i).
- A record is maintained by BBC logging all staff and pupil use of the Internet.

9. How will the Risks be Assessed?

It is difficult to completely remove the risk that pupils might access unsuitable materials via the school system.

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will supervise pupils and take all reasonable precautions to ensure that pupils only access appropriate material. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a computer terminal in school. The child turning off the monitor and informing a teacher immediately will deal with any instances. The teacher will then inform the ICT technician, who will contact BBC.
- Methods to identify, assess and minimise risks will be reviewed.
- Internet/Online Safety and rules are taught through Computing and PSHE lessons, as well as during Internet Safety Week and Online Safety activities.
- Internet Safety and SMART rules signed by each class annually and displayed in relevant classrooms.
- As part of the Online Safety/Computing lessons, pupils are taught about the dangers of online radicalization/extremism/terrorism and what to do if they have any concerns.
- Wearable devices such as Apple watches and dashcam use are covered in the Mobile Phone policy.

10. How will the School Ensure Internet Access is Safe?

Technical – infrastructure / equipment, filtering and monitoring
The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Following the guidance set out in 'Keeping Children Safe in Education' document 2023, we ensure appropriate filters and monitoring systems are in place and that children should not be able to access harmful or inappropriate materials in school. The internet is a communications medium that is freely available to any person wishing to send email or publish a website on almost any topic. Access to appropriate information should be encouraged and at PCA we are careful that 'over blocking' does not lead to unreasonable restrictions, however; Internet access must be safe for all members of the school community and we are aware the pupils must be taught how to use popular sites carefully, not shielded away from them.

- PCA technical systems will be managed in ways that ensure we meet recommended technical requirements
- There will be regular reviews and audits of the safety and security of technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to / academy technical systems and devices
- All visitors who wish to use PCA's Wi-Fi have to sign the PCA Public Acceptance Use Policy (see appendix iii)
- The "administrator" passwords for the academy ICT system, used by the Network Manager (or other person) must also be available to the *Headteacher* or other nominated senior leader and kept in a secure place
- The ICT Technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered (by Blackpool council and monitored and checked regularly by PCA) for all inappropriate online content including:
- Online bullying, child sexual exploitation, discrimination, drugs/substance abuse, extremism, pornography, self-harm and violence.
- Illegal content (child sexual abuse images, unlawful terrorist content or content with regards to female genital mutilation (FGM)) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- Technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person. Any internal incidents are reported to PCA's IT Technician, if there are any external incidents/cases of online bullying etc they are reported to PCA's Child and Family Support Manager/worker or Team Leader and evidence is collected where possible of the inappropriate behaviour. This is usually done by taking photo evidence of what has happened. These records are stored on CPOMS.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. PCA's infrastructure and individual workstations are protected by up to date virus software. PCA is protected by the Council's own firewall and all website traffic is filtered through FortiGuard Web Filtering software. All the computers have Windows Security installed for virus protection and the laptops have Norton Internet Security installed.
- As a rule PCA does not let hardware out of school for use with children, however there may be certain times when this may be allowed. All Teaching staff have work laptops/iPads and are bound by the same rules of conduct on their school laptop/iPad as they would be on a computer/iPad within the school setting. All staff are also issued with encrypted pen drives which they use if they want to store any pupil/personal information, photos or films.
- An agreed policy is in place that allows staff to /forbids staff from downloading executable files and installing programs on school devices. Staff are not allowed to run EXE files, this has been blocked from the server, only admin users with admin passwords are allowed to run EXE files on school machines. However, PCA laptops are not locked down to this.

11. How will we monitor online safety?

Following the guidance set out in 'Keeping Children Safe in Education' document 2023, we ensure appropriate filters and monitoring systems are in place and that children should not be able to access harmful or inappropriate materials in school.

- The IT Technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all inappropriate online content including: Bullying, child sexual exploitation, discrimination, drugs/substance abuse, extremism, pornography, self-harm and violence.
- Illegal content (child sexual abuse images, unlawful terrorist content or content with regards to female genital mutilation (FGM)) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- Technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement
- PCA uses the 'SHARP' system which is embedded on the school website. This stands for the 'Schools Help Advice Reporting System' where pupils or parents/carers can contact the PCA's behaviour co-ordinator. This can remain anonymous and is confidential. All reports are directly sent to the Deputy Head Teacher.
- When using the internet there is physical supervision of the children and staff will monitor screen activity.

12. How will Complaints Regarding Internet Use be Dealt With?

Parents may from time to time realise issues regarding the use of the Internet in school.

- These may be brought to the attention of the Headteacher or relevant others e.g classteacher/ Key Stage Team Leader etc. The Head and Computing Subject Leads may then work in partnership with the LEA to resolve such issues.
- If pupils are found to not be using the Internet responsibly, then sanctions include disallowing their use of the Internet for a fixed period of time and their parents being informed.

13. How will the Policy be Introduced to Pupils?

A SMART Rules poster will be displayed in each class base stating the rules for safe internet use.

The pupils will also read through a copy of these rules as part of Computing and PHSE work.

Internet Awareness lessons and safety lessons will be taught through Computing and PSHE and an annual Safety Internet Day.

14. How will the Policy be Introduced to the Staff?

Having written this policy, it will be e-mailed to all staff for a period of consultation. Following this it will be presented to the Governors for approval. Once it is in place, it will

be important for staff to familiarise themselves with the policy as we all hold a shared responsibility for the implementation of safe internet use by our pupils.

15. How will Parents' Support be Enlisted

A letter will be sent out at the beginning of each academic year briefly outlining the school's policy on Online Safety and also advising parents on the use of Online Safety and Social Media at home. Other information is provided via

- Letters, newsletters, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Regular National Online Safety (NOS) guidance in newsletters.
- Twitter
- Facebook

16. 'Responsible Internet Use' – PCA's Rules for Staff and Pupils

This document is on display in all rooms throughout the school. An age appropriate version of 'The SMART Rules' is also on display and signed in all classrooms for children's information (appendix ii).

"We grow together, we learn together, we will achieve our best together"

Headteacher: Mrs G Hughes
Deputy Headteacher: Miss H Gardiner

158 Whitegate Drive
Blackpool FY3 9HF
Telephone: (01253) 764130
Fax: (01253) 600670
Email Address: admin@park.blackpool.sch.uk
Website: www.park.blackpool.sch.uk

Dear Parent/Carer

At Park Community Academy our children are encouraged to use technology to support their learning and this may include the use of the Internet. We feel that access to such a large resource is very beneficial to support learning; however, we are aware that the Internet can also provide access to a variety of inappropriate material.

The school therefore has put in place a number of safeguards to ensure appropriate use of the Internet:

- All pupils read, discuss and sign a copy of our Online Safety Rules every year (please see overleaf)
- Pupils will only be allowed access to the Internet after being given instruction about responsible Internet use.
- All Internet use is filtered by Blackpool Borough Council and unsuitable sites are blocked.
- Internet access is always supervised.
- All pupils take part in regular online safety training.

I am sure that you will agree that when used correctly the Internet is an extremely valuable tool, however, if you have any concerns or issues about its use within school please feel free to discuss it with either of us.

Yours sincerely

C Johnson & A Brannigan
(Primary & Secondary Computing Subject Leads

PCA's Online Safety Rules

Online Safety Rules

S

Safe
Keep safe. Never tell anyone on the internet your full name, address or your telephone number.

M

Meeting
Never meet up with anyone you meet on the internet. If someone asks you to meet them tell an adult.

A

Accept
Never accept emails or text messages from people you don't know.

R

Reliable
Never rely on what you read on the internet, it isn't always true. Don't rely on people on the internet, they may lie to you!

T

Tell someone
Always tell an adult if something you see, read or hear on the internet upsets you.

"We grow together, we learn together, we will achieve our best together"

Headteacher: Mrs G Hughes
Deputy Headteacher: Miss H Gardiner

158 Whitegate Drive
Blackpool FY3 9HF
Telephone: (01253) 764130
Fax: (01253) 600670
Email Address: admin@park.blackpool.sch.uk
Website: www.park.blackpool.sch.uk

PCA Internet Access – Public Acceptance Use Policy

- The computer system is owned by the Academy and is made available to pupils to further their education and to staff to enhance their professional activities including teaching.
- The PCA Internet Access Policy has been drawn up to protect all parties – the students, staff visitors/public and the Academy.
- PCA reserves the right to monitor any internet sites visited.
- All internet activity should be appropriate to be professional activity or to the education of students.
- Access should only be made through the authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- Misuse of equipment or unsafe practices must be reported to the computing technician.

Please sign below to acknowledge that you understand and agree to the above terms

Full name……

Designation……Date……

This password will expire after two hours. Please use the same network code and password if you need to log in again during your visit. Username and passwords are case sensitive