Palmers Cross Primary School

E-Safety Policy

Reviewed: June 2015

School Vision

Palmers Cross embraces the idea that technology is now considered, to be an essential part of modern life, and that the school has a duty to provide pupils with quality technology as part of their learning.

This E-Safety Policy considers the use of range of current technologies and will be revised to incorporate new and emerging technologies as they appear. It will include reference to all stakeholders, including learners, school staff, governors and parents/carers.

The purpose of technology use in school is to help deliver the whole school aims i.e. to offer a curriculum that is enhanced by integrating Computing across all subject areas (e-learning), promoting enjoyment, a personal sense of fulfillment, achievement and the life skills that will help our children thrive in the 21st Century.

As the uses of online technological resources grow, so has the awareness of risks and potential dangers which arise for their use. This school aims to prepare its learners to be able to thrive and survive in this complex digital world. This policy outlines the safeguarding approach to achieve this.

Writing and reviewing the E-Safety Policy

This policy is also linked to other policies including those for Computing, bullying and for child protection.

- Our E-Safety Policy has been written by the school, building on the local authority Digital Safeguarding Policies and Government guidance. It has been agreed by the Leadership Team and approved by the IEB.
- The E-Safety Policy and its implementation will be reviewed annually.
- The E-Safety Policy was revised by:
- It was approved by the Interim Executive board on: 5th August 2015

Equality and inclusion

The use of technology is a part of the statutory curriculum and a necessary means of delivering 21st Century teaching and learning for staff and pupils. Internet access is an entitlement for all. However, responsible and safe use must be at its core.

Management of E-Safety

All school stakeholders within the school are required to sign an AUP (acceptable use policy) for technology. This includes pupils, members of the workforce, governors, parents and carers. (See appendix 1). All staff have an e-safety responsibility, and should be kept regularly fully aware of e-safety issues and should demonstrate and model good practice. E-safety is seen as a priority within school and across all curriculum areas, and as such staff receive appropriate and regular training. At Palmers Cross, we value the contribution of the wider community to e-safety, and ensure that our ethos, policy and practice are shared and involves all stakeholders

Procedures for reporting

At Palmers Cross, we ensure that our reporting and recording routines are understood by all stakeholders, particularly how and to whom a learner should report concerns. Our e-safety reporting procedures are encompassed by wider safeguarding reporting procedures and any incidents are reported to the nominated E-Safety Leader in the same way as a normal safeguarding issue. This will then be passed on to the person in charge of safeguarding and dealt with in line with the school safeguarding policy. **(See Safeguarding Policy).** Any such incident will be dealt with swiftly and support offered to all parties involved.

Clearly stated roles and responsibilities

- Head of School

The Head teacher will ensure that the E-Safety Policy is implemented and compliance with the policy monitored, and that the appropriate roles and responsibilities of the school's e-safety structure is in place.

- Nominated E-Safety Leader

There is an identified E-Safety Leader who is responsible for e-safety developments in school and sharing of practice with staff and the wider community. This person will receive current high level training and on the latest guidance and procedures and is the main contact for the central e-safety networks. All e-safety incidents within the school should be reported to this person. They will keep the log of incidents and with the Head of School make decisions about how to deal with reported incidents.

- E-Safety IEB member

There is an identified E-Safety IEB member who monitors and liaises with the E-Safety Leader and who will report to full governing board as appropriate.

- E-Safety responsibility within subject and management roles

All staff with subject and management roles have a duty to incorporate e-safety principles in their area of responsibility, deputising for any of the above roles where appropriate.

- Teacher

All staff understand the need for care and caution when using technology both for academic and social purposes and apply it to teaching and learning situations. They need to work to agreed guidelines (e.g.

Communications Technology Staff AUP) and understand the potential repercussions of non-compliance. They have a "front line" monitoring and reporting role for incidents.

- Support Staff

As for teaching staff, support staff should be clear of the reporting procedures and their roles and responsibilities.

- School Council representatives

As a responsible member of their class the school council may have e-safety as a regular agenda item. These representatives could help to monitor at a learner level the appropriate use of technology within the school.

Teaching and Learning

At Palmers Cross Primary School we ensure that we deliver an age-appropriate, flexible yet robust e-safety curriculum integrated into other curriculum areas as appropriate. We ensure that we teach our learners how to stay safe in their use of technology, how to protect themselves and how to take responsibility for their own safety. We use a range of resources such as …. www.thinkuknow.co.uk

www.ceop.police.uk

www.bbc.co.uk/cbbc/topics/stay-safe

www.hectorsworld.com

www.kidsmart.org.uk

Our e-safety curriculum is dynamic (responds to changes in trends and technology) and planned carefully to ensure that all learners are able to access it in an appropriate way.

Involving parents and carers

At Palmers Cross Primary School we believe that it is vital to involve parents and carers in the e-safety process, ensuring that both they and their children are able to stay safe and conduct themselves appropriately in the digital world. In order to achieve this we aim to regularly involve parents/carers in 'workshops' and meetings to inform them of potential dangers of the internet including social networking websites such as Facebook.

Risks and acceptable Behaviours

- Use of the internet

The internet is a vital tool to be used inside and outside of school. However at Palmers Cross Primary School there are procedures put into place to ensure appropriate use. When all children start at Palmers Cross Hall Primary School they are required to sign an AUP (agreement) appropriate to their Key Stage, which refers to appropriate internet use.

- Passwords/personal details

Both children and staff are given passwords and logon details to access the school system and learning platform. Staff will be encouraged to personalise their password and change it regularly. Children are encouraged to report any occasions when their password may have been compromised so that it can be re-set accordingly.

This policy should be read in conjunction with our Data Protection Policy which identifies the school's responsibilities in terms of data.

- E-mail

Staff must use their school provided email account rather than a personal account for school business. We also recommend staff to not email files that contain any details of pupils, using the learning platform as an alternative.

- Learning Platform

The Learning Platform is widely used by staff, children and governors. To ensure digital safety, all users have a personal logon and password that is unique. All users are encouraged not to share their details with anyone particularly when out of school setting. Each year group site should have a set of class site rules outlining how children should conduct themselves.

- Appropriate use of hardware

Staff will be given appropriate training when they receive a new piece of hardware. They are asked to sign a laptop agreement (appendix 2) when they begin employment at the school. All staff devices must have an appropriately strong password (including iOS devices which can be changed to have an alpha-numeric password instead of the default 4 digit).

- Photographs, video and sound recording

All children are required to sign consent form (appendix 3) that allows them to be photographed and recorded whilst at Palmers Cross Primary School. If children are not allowed, then relevant staff will need to be aware and ensure that this is adhered to. A list of those children whose images are not allowed to be used is stored centrally. When using digital cameras or video cameras, we insist that:

  - Staff never use a personal device to record images of children
  - When a school device is used, images/ videos are taken from the device as soon as possible

- Copyright

Copyright is an essential part of e-safety: at Palmers Cross and staff and learners (at an appropriate level) are made aware of their responsibilities to copyright and potential copyright issues through regular training/ curriculum opportunities. At Palmers Cross Primary School we provide alternative resources and information to enable staff and learners to create content without contravening copyright. For example, sites such as Espresso or www.freeplaymusic.com (for educational, in-class use). For further detail, see the attached copyright statement (Appendix 4).

- Data Security

We discourage the use of memory sticks especially if they contain sensitive information about children e.g. photographs or personal details. Rather than memory sticks staff are recommended to use the Learning Platform for data storage and security. We recommend that no images of children, data about children or any personal files on their laptops. All sensitive data/ media of this kind will be saved either on the learning platform or server.

Staff:

At Palmers Cross Primary School, we acknowledge the prevalence of social networking, and that it plays a huge part in today's society. However, it is vital that staff conduct themselves professionally and appropriately within these environments. All staff are made aware of the Local Authority HR view regarding acceptable behaviour (See Grey Book) - staff should not make any reference to their job, school or other colleagues on the site and should not accept friend requests from current or former pupils under 18 years of age. We also ensure that staff are fully aware of the potential consequences should this be contravened.

Learners:

We recognise that the minimum age on many social networking sites is 13 and actively advise our learners from creating accounts. We are, however, aware that where this advice is not followed, we have a duty to equip our learners with the knowledge and understanding required to keep themselves safe online. We also advise parents of steps they may take to help keep their child safe on social networking sites.

Any disclosures made regarding cyber bullying or inappropriate conduct or contact that occur either within or outside school should be reported and dealt with in line with the school's anti-bullying policy and/or safeguarding policy. School resources such as US-Online, Kidsmart and CEOP's 'U think U Know' all contain activities for both key stage 1 and key stage 2 children that discuss and highlight how to be safe when on social networking sites.

- Mobile phones/technology

Children are not allowed to bring mobile phones into school. Staff can use mobile phones outside lesson time. We ensure that all staff do not use their own devices to capture images of learners and that images are always taken off the school devices as soon as possible.

Impact and monitoring

The effectiveness and impact of this policy may be measured in the following ways:

- Incident log
  - All incidents of an e-safety nature will be reported in the same manner as other safeguarding incidents. An online e-safety incident form will be completed on the staff site of the learning platform. Monthly statistics will be reported to the Head Teacher by the E-Safety Leader.
- Minutes of school council
  - E-Safety will form part of the regular agenda and subsequent discussions will be minuted.
- Regular analysis of systems, resources and curriculum to adapt to changes in online behaviour and the emergence of new technologies.

Links to other school policies/school documents

This E-Safety Policy will be linked to the following:

- Strategic ICT plan
- Curriculum policy
- Reference in other school policies
  - Anti-bullying
  - Safeguarding
  - Data Protection
  - PSHE
  - Computing
  - EYFS
- Critical Incident policy
- Wolverhampton Grey Book
- School website

This policy will be reviewed annually.

Written by:		Date:	
Agreed by Governors:		Date:	

Communications Technology Staff Acceptable Use Policy

The policy aims to ensure that any communications technology is used without creating unnecessary risk to users while supporting learning.

I agree that I will:

- only use personal data securely
- implement the schools Computing and E-Safety policies
- educate pupils in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- educate pupils in the recognition of bias, unreliability and validity of sources
- actively educate learners to respect copyright law
- only use approved e-mail accounts in school
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified
- only give access to appropriate users when working with blogs or wikis etc…
- set strong passwords – a strong password is one which uses a combination of letters, numbers and other permitted signs
- report unsuitable content or activities to the E-Safety Leader
- ensure that videoconferencing is supervised appropriately for the learner's age
- read and sign the Acceptable Use Policy
- pass on any examples of Internet misuse to a senior member of staff
- post any supplied E-Safety guidance appropriately
- think carefully about what is stored on my laptop and make efforts to store sensitive data on the school server or private area on the Learning Platform

I agree that I will not visit Internet sites or make, post, download, upload or pass on: material, remarks, proposals or comments that contain or relate to:

- pornography (including child pornography)
- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting illegal acts
- breach any Local Authority/School policies, e.g. gambling
- do anything which exposes children to danger
- any other information which may be offensive to colleagues
- forward chain letters
- breach copyright law

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

Name …………………..……………………………….. **Date** ………………………………

Governor Acceptable Use Policy

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to support management and learning without creating unnecessary risk to users.

(1) Management Role:

As an IEB member, I will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an e-safety leader and a named governor takes responsibility for e-safety
- an e-safety policy has been written by the school, building on Wolverhampton's LA e-safety (Digital Safeguarding) example and relevant guidance
- the e-safety and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is understood and not breached
- learners are taught to evaluate digital materials appropriately
- parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URLs and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology (using the Self-Review Framework) to establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff

(2) Accessing and/or Using School/Local Authority IT Systems and Facilities

As a IEB member, I agree that I will:

- only use personal data/sensitive personal data securely
- adhere to the school's e-safety policy
- only use secure e-mail accounts when dealing with school personal data/sensitive personal data
- set strong passwords (using a combination of letters, numbers and other permitted signs)
- not reveal my password to anyone
- inform the Head of school immediately if I believe someone else may have discovered my password
- report any security concerns to the Head of School as soon as possible
- observe security guidelines at all times
- only store school personal data/sensitive personal data on the school server or private area on the school's learning platform, not on my personal computer/laptop/portable device
- not attempt to access any of the school's/LA's facilities using anyone else's login details
- not introduce or attempt to introduce any form of malicious software onto the school's/LA's management information system or learning platform
- not change or attempt to change or remove any part of the school's management information system or learning platform
- not deliberately delete files from the school's management information system or learning platform
- not edit, alter or use on any other website or social network site, any downloaded images or video obtained from the school's site.

I agree that, when using school and/or local authority facilities, I will not visit internet sites or make, post, download, upload or pass on material, remarks, proposals or comments that contain or relate to:

- pornography (including child pornography)
- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting illegal acts
- breach any Local Authority/School policies, e.g. gambling
- do anything which exposes children to danger
- any other information which may be offensive to colleagues
- forward chain letters
- breach copyright law

I accept that my use of the school and/or Local Authority IT facilities may be monitored and the outcomes of the monitoring may be used.

I agree to the terms and conditions above.

Name: ………………….…………………………………………………

Signature: ……………………………………………………………….

Date: ………………………………………………………………………

Schools Laptop Agreement

This document is an agreement between both staff and school, and shall be binding for the duration of employment at the school.

General

1. The laptop shall remain the property of the school.
2. The laptop shall be retained by staff in order to exercise their professional duties.
3. The laptop shall be returned to school upon a member of staff leaving school to take up a post elsewhere and any additional software/saved data removed.
4. Staff are to take proper care of the laptop at all times.
5. Staff shall be responsible for the security of the laptop, ensuring it is in a lockable cupboard when unattended in school and ensuring all reasonable precautions are taken when transporting the laptop.
6. Any additional software installed on the laptops is to be correctly licensed.
7. All faults are to be reported to the Computing Leader/Technician.
8. Any loss, theft or data breach will be notified to the nominated E-safety leader immediately

Use

1. The laptop shall be available for use in school each day.
2. Staff shall be aware of the issues relating to access to Internet sites not relevant or appropriate to their professional duties.
3. Staff shall operate Internet access with due regard to school and Wolverhampton City Council policies.
4. Staff shall use the laptop in a responsible and professional manner.
5. Staff will be expected to use the laptop for:

- Planning
- Delivery of lessons
- Record keeping
- Analysis of assessment
- Target setting
- Accessing Learning Platform
- Other professional duties

The school agrees to provide training for teachers in order to make effective use of their laptop.

I …………………………………………………. agree to the terms and conditions above.

Signed ………………………………………………

Laptop Info

Date	Model	Service Tag	Orange Sticker