ICT, SAFER INTERNET AND E-SAFETY POLICY

FOR SCHOOLS WITHIN

THE KEYS FEDERATION ACADEMY TRUST

St. Peter’s C. of E. Primary School, Hindley
Hindley Green Community Primary School
St. John’s C. of E. Primary School, Hindley Green
St. John’s C. of E. Primary School, Abram

September 2018

Writing and reviewing our ICT policy:

Our ICT Policy has been agreed by all four schools building on LA and government guidance. It relates to other policies including those for bullying and Safeguarding & Child Protection. It has been agreed by our senior leadership teams, our staff and approved by our Board of Directors in the **Autumn Term 2018**. The Trust's ICT Policy will be reviewed annually, will be available on the staff drive in each school and its importance will be explained and regularly referred to.

Our Vision

Computing is an essential key to the success of our 21st Century Learners. Our schools act as focal points for the wider community, with great emphasis placed on life-long learning. Advances in technology will be embraced by all of our learners, including our adult learners, because we are responsible for engaging and motivating our learners to create a cohesive community both in the real and virtual worlds.

General Data Protection Regulation (GDPR)

Computers have been provided by The Keys Federation Academy Trust for use by staff as an essential tool for teaching, learning and administration of the Trust and its schools. Use of Trust computers, by both members of staff and pupils, is governed at all times by this policy and the General Data Protection Regulation. It is important that staff understand their responsibilities under this policy and direct any questions or concerns to the Trust Data Protection Officer in the first instance.

All members of staff have a responsibility to use the Trust's computer system in a professional, lawful and ethical manner. Deliberate abuse of the Trust's computer system may result in disciplinary action.

1. Leadership & Management

Within all schools our Skills/ICT Teams oversee the strategic planned development within our schools. The Teams are responsible for moving our schools forward and ensuring support is in place to develop staff capabilities in the continually developing field of Computing. Our ICT Team Leaders will attend relevant courses to enable them to steer and lead the school's developments with regard to the latest technological advancements.

The Team Leaders will **not** act as a technician, but will advise colleagues on managing equipment and software. The responsibility for the maintenance will fall with the provider of the Service Level Agreement (SLA), currently Abtec Computer Services. All faults must be reported to the ICT Team Leaders via the preferred method of reporting issues in each school. The ICT Team Leaders will ensure that the technicians are contacted to resolve the issues. Any decisions with regard to replacements must be agreed by the Federation Executive Team.

→ 1.1 E-Safety & Online Protection

All computers within schools are fitted with a recommended e-safety software package. Apple I-pads/I-pods are filtered through the server. This will allow the Principal, as Designated Safeguarding Lead, and the SLT to monitor the appropriate use of ICT equipment within schools. All staff, learners and families within our schools are made aware of this software and its usage and all incidents will be dealt with using the appropriate procedures to safeguard children (Please refer to **Appendices 1 & 2)**.

Staff will be aware that all users of the school's systems **must** use their personal account because all digital traffic is monitored and traced to the individual user. Discretion and professional conduct is essential. Learners will be informed that network and Internet use is monitored by e-safety Software.

E-safety rules will be posted in all wireless active rooms and discussed with the learners at the start of every year and at regular intervals.

All schools have the Tootoot reporting system as one medium for reporting safeguarding issues.

All pupils are taught to handle hardware correctly and to access software and the internet safely (Please refer to **Appendix 3**), as well as due adherence to health and electrical safety when switching computers on and off using the correct procedures.

Parents'/Carers' attention will be drawn to the ICT Policy and e-safety in newsletters, the school prospectus and on the school website.

→ 1.2 Authorising Internet access

- All staff must read and sign the 'Acceptable Use Agreement' before using any school ICT resource, along with the LA's Guidance for Schools on Acceptable Use of IT.
- Parents/Carers will be asked to sign and return an Internet Access consent form and an 'Acceptable Use Agreement' with their child(ren).
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance staff may have temporary access, a member of staff may leave or a pupil's access be withdrawn.
- In our Early Years Foundation Stage and Key Stage 1 departments, access to the Internet will be by adult demonstration with supervised access to specific, approved on-line materials e.g. Purple Mash

→ 1.3 Sanctions for Mis-Use

Any breach of our Acceptable Use Policy will be considered a serious risk to health, safety and security (Please refer to **Appendices 4, 5, 6 and 9)**, and will lead to the following: Access is seen as a privilege, not a right and that access to the Internet requires responsibility.

- An incident review meeting with a member of our school's SLT.
- Temporary or permanent bans on Internet access and learner's parents/carers will be informed. Serious breaches in internet use may be considered as a 'Child Protection' concern and as such, advice may be sort from the Wigan Safeguarding Children Board.
- All major incidents will be catalogued and reported to our Board of Directors and for the purpose of criminal investigations.
- Parents/Carers will be expected to promote safe and secure online activity with their child(ren).
- In the case of employees, any breach may also be considered a breach of the employee's conditions of service which could lead to appropriate disciplinary action including dismissal on grounds of gross misconduct.

→ 1.4 Managing filtering

- ♦ The school will work with Wigan LA and the Internet Service Provider to ensure systems to protect learners are regularly reviewed and improved and are appropriate for filtering and monitoring in educational settings. See guidelines from the UK Safer Internet Centre.
- ♦ If staff or learners discover an unsuitable site, either when performing internet searches or when accessing links within sites, it must be reported to the E-Safety Co-ordinator/Principal.
- ♦ SLT staff and ICT maintenance staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

→ 1.5 Managing videoconferencing & webcam use

- ♦ Videoconferencing should use the educational broadband network to ensure quality of service and security. Alternatively, SKYPE permissions can be sought and approved via Abtec.
- ♦ Learners must ask permission from the supervising teacher before making or answering a videoconference call.
- ♦ Videoconferencing and webcam use will be appropriately supervised for the learners' age.

→ 1.6 Managing emerging technologies

- ♦ Emerging technologies will be examined for educational benefit and, where necessary, SLT's will undertake a risk assessment before use in schools is allowed.
- ♦ All mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- ♦ Learners are required to hand in all mobile phones and handheld devices at the start of the school day. They will be securely stored in the school's offices and returned to learners at the close of school.
- ♦ Devices that can bypass our school's filtering systems will be carefully monitored by SLT and all staff.

2. Professional Development

Regular staff meetings and/or Spirit of Purpose sessions will be arranged for staff to work on Computing. This will include:

- E-safety Training provided by CEOP
- Development of Online Learning Spaces
- Introduction to new software/sharing ideas
- General training for ICT procedures
- Whole school support in planning for Computing
- Moderation of children's work for our Computing e-portfolio
- General Data Protection Regulations

All staff will attend relevant training, identified as an aspect of Performance Management, and have opportunities to work alongside other professionals through Peer Coaching sessions within our schools. ICT Co-ordinators will also complete on-line e-safety training.

3. Curriculum

Computing will be integral and used as a tool to enhance all other areas of learning. In addition, we aim to promote the skills and knowledge of Computing as a subject in its own right. Computing capability will be delivered though the progression of skills based on the National Curriculum programmes of study and level descriptions. E-safety will be embedded within the Computing scheme of work and the Personal Social and Health Education (PSHE) curriculum using a range of materials suggested on the CEOP website.

→ 3.1 Skills and knowledge

We aim to:

- promote and develop confidence and proficiency in the use of ICT in all learners, including adult learners.
- develop an appreciation and proficiency in the use of ICT in the context of the wider world.
- promote the enrichment of learning, self-led study and collaborative work.
- develop the ability to use ICT appropriately and to choose software suitable for a particular task.
- promote Computing skills through contexts for learning.

- encourage problem solving and investigation.
- ensure that provision for the development of ICT has a strategic focus to ensure future advances are catered for.
- provide continuity and progression in the strands of the Computing National Curriculum.
  - ❖ Communication and Handling Information – using ICT to generate and communicate ideas in written, visual or aural forms and to retrieve, analyse and amend information. This will include communication via email and the Internet for research.
  - ❖ To develop the use of communications beyond the schools (e-mail, video-conferencing and Virtual Learning).
  - ❖ To develop the use of the Internet as a data/research and communication tool.
  - ❖ Control and Monitoring – using ICT to control and monitor external events.
  - ❖ Modelling – to explore computer representations of ideas and of real and imaginary situations

4. Teaching and Learning

The Internet is an essential element in the life of our 21st century learners - for education, business and social interaction. The schools have a duty to provide our learners with quality Internet access as part of their everyday learning experiences. The Internet is a part of the statutory curriculum and a necessary tool for staff and learners.

Activities will be planned and targeted according to each learner's individual and different needs, building on their previous learning and skills and giving learners opportunities to apply their skills in different contexts.

Computing will be delivered through a variety of teaching and learning methods e.g. whole class, group and individual work. Differentiation and progression is ensured by a variety of approaches such as:

- Same activity but different expectations of outcome.
- Same theme, but different levels of input.
- Allowing for different pace of working.
- Different groupings of learners.
- Use of Junior Digital Leaders to promote peer to peer learning.

→ 4.1 Internet use will enhance learning

- ♦ Our school Internet access is designed expressly for learner use and will include filtering appropriate to the age of learners.
- ♦ Learners will be taught about acceptable and appropriate Internet use and they will be given clear objectives for Internet use.
- ♦ Learners will be educated in the effective use of the Internet to support their research, including the skills of knowledge location, retrieval and evaluation.
- ♦ Learners will be shown how to publish and present information to a wider audience.

→ 4.2 Learners will be taught how to evaluate Internet content

- ♦ Learners should not be allowed to use sites such as Google to search for images unless under the direction of the teacher during research sessions. **Results of searches must always be checked by staff prior to classroom use**.
- ♦ Our schools will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- ♦ Learners will be taught to be critically aware of the materials they read and will be shown how to validate information before accepting its accuracy.

- ♦ Learners will be taught about responsible online activity and about how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.
- ♦ Learners are responsible for good behaviour on the Internet just as they are in a classroom or when representing the schools in any way. General school rules apply.
- ♦ Outside of school, families bear responsibility for guidance as they must also exercise with information sources such as television, radio, newspapers, magazines, telephones, films and other potentially offensive material.

→ 4.3 Social networking and personal publishing

- ♦ The school will block/filter access to social networking sites.
- ♦ Newsgroups will be blocked unless a specific use is approved.
- ♦ Learners will be advised never to give out personal details of any kind which may identify them or their location.
- ♦ Learners and parents/carers will be advised that the use of social network spaces outside school is inappropriate for primary aged learners- see social networking advice attached.
- ♦ Staff will adhere to guidelines within the LA Social Medial Policy for employees (attached).
- ♦ Safe use of the internet including social networking is a key priority for all our users. The safe use of social networking will form a key part of our e-safety workshops.
- ♦ Sexting is clearly an area of concern for all those under the age of 18 and guidance in the form of 'Sexting in schools and colleges: Responding to Incidents and Safeguarding Young People' (September 2016) is provided for Designated Child Protection Officers, school leaders and teachers. This document should be available in schools as an integral part of the Safeguarding and Child Protection policy.
- ♦ 'Tootoot' has been introduced to each of our schools as a reporting tool that allows children to raise any concerns regarding cyber bullying, grooming, sexting or extremism via an online platform. Children have been introduced to this service and provided with log in details. Each school will have a minimum of two administrators who will receive alerts regarding direct reports and can address these appropriately, using our safeguarding guidelines. All reports are recorded allowing schools to monitor these incidents and their outcomes.

→ 4.4 E-mail

- ♦ Learners and staff may only use the designated e-mail accounts on the school systems. All other e-mail accounts are prohibited.
- ♦ Learners will immediately inform a member of staff if they receive e-mail that they consider to be offensive.
- ♦ Learners will ensure that personal details about themselves or others are not included in any e-mail communication and learners will be taught not to use e-mail to arrange to meet anyone.
- ♦ All e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- ♦ The forwarding of chain letters is not permitted.

→ 4.5 Individual and Different Needs

Our schools recognise the advantages of the use of ICT by learners with individual and different needs. Using ICT can:

- Address learner's individual needs
- Increase access to the curriculum
- Enhance language skills
- Provide tools to deliver interventions to those pupils with specific needs.
- Provide a greater level of challenge for more able learners

- Allow demonstration of their skills and talents

→ 4.6 Time Allocation

All classes will have regular access to ICT (Laptops/I-pads/Asus/Video Conferencing/Digi-Blues etc). Further opportunities to develop and extend Computing capability will be provided by the use of laptops to support continuous provision.

→ 4.7 Equal Opportunities

Our schools promote equal opportunities for computer usage and fairness of distribution of ICT resources. Where learners cannot access ICT at home, school will provide opportunities outside of normal school hours, i.e. lunchtimes or after school.

5. Resources

The school resources include:

- Calculators
- Computers/Laptops
- Access to email and internet
- Scanner
- Digital cameras/ WebCams/Camcorder
- Apple I-pods and I-pads
- Roamers/Beebots/Probots/Lego Mindstorms
- Television and DVD/videos
- Hand held dataloggers
- Video conferencing facilities
- Blog site
- Visualisers

Please see separate audit for full resource list as these are developing annually in each school.

Staff will organise their online spaces and resources in such a way that point learners to sites/links which have been reviewed and evaluated prior to use. While learners may be able to move beyond these resources to others which have not been evaluated by staff or recognised providers, learners will be provided with guidelines and lists of age appropriate resources particularly suited to the learning objectives.

All learners will be informed of their rights and responsibilities as electronic resource users before their first use. To enable learners to conduct research and complete their studies and tasks, staff will give regular reminders about acceptable use referring to our e-safety rules, which should be displayed in every room where learners access ICT.

→ 5.1 Software

A list of available software is kept within each school. All individuals have access to software that is relevant to them by logging onto our servers. **Any software that does not have a site licence must only be installed on the individual class laptop only**. Our maintenance provider, Abtec, is responsible for the installation of software onto the school servers.

→ 5.2 Network Access Control

In accordance with Financial Regulations, ICT auditors will have access as necessary to any information and applications systems. Any method of log-on which nullifies the password control is prohibited.

Every user will have an individual username and password. The use of another person's username is strictly prohibited. Passwords must not be printed, displayed on input or disclosed to anyone else.

Passwords must be changed immediately if it is suspected that the password has been disclosed. Access rights for all leavers will be removed immediately. Access rights for all users should be reviewed and updated periodically.

→ 5.3 Equipment Security Procedures

The Principals are responsible for all ICT facilities installed within our schools and for ensuring their proper use. The use of ICT facilities not directly concerned with our School's business is prohibited. All items of equipment must be security marked in accordance with the School's risk management policies and included on the inventories. The schools have an alarmed system installed throughout. The Servers are stored in locked rooms each night. The school's laptops and other Mobile Technology are stored in locked central/classroom cupboards.

Equipment must only be kept in secure areas, not able to be accessed by members of the public or unsupervised representatives of other organisations. Where equipment is located within central areas and can be accessed by members of the public or in unsecured offices and left unattended for periods of time, the following measures will be considered to deter the theft of that equipment:

- Steel cable attachments locking equipment to the work surface
- Improved security of the outer walls and windows
- Intruder alarm

Laptops must not be left unattended when logged in to applications. If not in use they must be logged out or protected by a secure screen saver. Users must log out of the systems and the network before signing out of work and also switch off all electrical equipment.

→ 5.4 Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Sophos Anti-Virus protection will be updated regularly.
- Security strategies will be discussed in relation to Wigan LA IT Security guidelines attached.

→ 5.5 Portable Resources

The permission of the Principal must be received before any loaned equipment leaves the school building. The removal of equipment should be recorded and monitored with records for equipment 'on loan' stored in the main admin Office. Equipment must not be left in unattended vehicles for which insurance is not available.

All staff laptops to support Teaching and Learning activities will be loaned to members of staff following completion of a signed agreement of long term loan. Unlicensed, illegal or unauthorised software or information must not be installed, used, copied, altered or distributed. Illegal or improper access to external networks, services or facilities is prohibited. (Please refer to **Appendix 7**).

→ 5.6 Disposal of Obsolete Resources

The disposal of obsolete computer equipment is governed by The Keys Federation Scheme of Financial Administration (SOFA). The Board of Directors should authorise all write offs and disposals of surplus stocks and equipment in accordance with DfE regulations. All information should be physically deleted, corrupted or overwritten so as to make it irrecoverable. Software is not offered to an external agency unless there is a legal right to do so and licence records are adjusted accordingly. Office /Estates staff ensure inventories on Parago are updated to record the disposal.

6. Assessment

Assessment for learning will be carried out by teachers in the course of each unit of study. This assessment may focus on:

- Discussion of the features of the software used.
- The outcomes of work assigned to our learners.
- Strategic questions to monitor understanding of skills and their application.

Learner attainment is assessed and recorded every term on our Computing Key Skills Tracking sheet.

ICT leaders will monitor learners' digital work and compile a portfolio of evidence to celebrate impact. Each half-term different learners will be selected to participate in pupil voice interviews about their Computing work to ensure consistency and continuity across the school. Feedback will be given to SLT and staff re: peer coaching opportunities and up-levelling learners' work.

Evidence of assessed work is stored on the servers and learners can retrieve work from their personal space on our school networks.

Parents/carers will receive a written report on all aspects of the learner's work as part of the annual report sent out at the end of the Summer Term every year.

→ 6.1 Definition and Classification of Information

Within this Policy 'information' is defined as data, programs, documents, spreadsheets, databases, electronic mail messages, images and maps of all types regardless of how or where within the Schools the information is stored or managed.

→ 6.2 Information Backup

The Principals/Federation Executive and Senior Leadership Teams must make sure that appropriate procedures are in place to maintain the confidentiality of the information and to recover from the temporary or permanent loss of the information or supporting equipment.

All information must be protected by a procedure for archiving and copying for security backup. The procedure must incorporate daily, weekly, monthly, year end cycles appropriate to the type of information, frequency of update, legal and operational requirements.

Security back up copies, when used, will be stored wherever possible off site from the location at which the operational information is maintained. The ability to restore information from back-up copies must be tested periodically by the ICT Maintenance Provider, to ensure that procedures, equipment and storage media are performing correctly.

→ 6.3 Compliance with Legal Requirements

All ICT data must be stored and disposed of with due regard to its sensitivity and the requirements of the General Data Protection Regulations. Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations.

7. Publishing Material Online

Our school's websites can be accessed by anyone on the Internet. A web page can celebrate good work, promote the schools, reflect recent and future school events, publish resources for homework or projects and highlight other sites worth visiting.

→ 7.1 Published content on the school websites

- Our Principals and SLT will take overall editorial responsibility, however all staff are responsible for ensuring that content is accurate and appropriate.
- The web page will comply with our schools and the DfE guidelines for publications.
- The contact details on our school's websites will be the school addresses, e-mail and telephone numbers. Staff or learners' personal information will not be published.

→ 7.2 Publishing learners' images and work

- Learners will be taught to publish for a wide range of audiences including Directors, parents/carers, prospective parents/carers, past learners or younger learners.

- Photographs that include learners will be selected carefully and will not enable individual learners to be clearly identified.
- Learners' full names will not be used anywhere on the website or Blog, particularly when attached to photographs.
- Parents/Carers are asked to sign a GDPR and Photography Consent Form which covers use of the Internet on entry to school before photographs of learners are published on the school website (Please refer to **Appendix 8**)
- Learner's work can only be published with the permission of the learner and parents/carers. All material must be the author's own work, credit other work included or accessed and state clearly the author's identity or status.

8. General

8.1 Community use of the Internet

- The schools will liaise with local organisations and educational establishments to ensure a common approach to e-safety.
- All temporary users (including staff from other establishments, regular supply staff, parents/carers etc) will be allowed to have access to the school systems using individual usernames and passwords.

8.2 Assessing risks

- The schools will take all reasonable precautions to ensure that users only access appropriate material.
  However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- Neither the schools nor the Academy Trust can accept liability for the material accessed, or any consequences of Internet access.
- The schools will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

8.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a member of SLT.
- Any complaint about staff misuse will be referred to our Principals.
- Complaints of a child protection nature will be dealt with in accordance with the Trust's Safeguarding and Child Protection procedures.
- Learners and parents/carers will be informed of the Trust's Complaints Procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

8.4 Class Dojo

Class Dojo is a communication tool for staff to communicate with parents/carers. See appendix 10 for guidelines of acceptable use of this tool.

8.5 Acceptable use of PTA Facebook page

In this digital age, parents/carers' use of technology is increasing. To maximise and market school events, PTA's are using social media more frequently. See appendix 11 for guidelines of acceptable use of Facebook in this way.

8.6 Staff APP

As a means of electronic communication, staff are required to download The Keys Federation APP on a compatible device. This APP is GDPR compliant.

This Policy was reviewed with due regard to the Equality Act 2010 and was presented and approved by Directors during the Autumn Term 2018. This policy will be reviewed every year to ensure that our schools continue to be at the leading edge of digital advancements.

Signed: *S. Bruton* CEO