# Kensington Avenue Primary School and Children's Centre

## Computing Policy and Procedures October 2017

**Kensington Avenue Primary School's (KAPS) Computing Policy has been written taking advice from many different local authorities and other schools** and aims to meet the criteria established by organisations such as Becta, 360Safe and ICT Mark.

**This policy has been written with a Creative Commons license in mind, meaning that you can use this in your school and adapt it but please send us an email if you have any suggested improvements or comments.**

**This policy was agreed by Governors in July 2013 and will be reviewed annually to take into account changes to practice, guidance and statutory duties that need to be made.**

**The definition of 'Staff' referred to in this document means all adults, including supply staff, teaching students and volunteers. The ICT Manager will ensure that all sections of the school community understand the purpose and scope of the Acceptable User agreements in relation to the e safety policies and that this is part of the school's induction procedures. It is the responsibility of the Head teacher to ensure that the processes contained within this policy are adhered to and with due regard to consistency and fairness in their application.**

**Review date: October 2018**

**Contents Page – (**Press Ctrl and click a link to view its contents**)**

**Introduction**

This policy covers the different elements of Information Communication Technology (ICT) used within our school. These guidelines have been drawn up to ensure that all stakeholders within the school are aware of what is expected of them and are able to stay safe when using the hardware and software linked to school and home. The equipment and resources within school are provided to enhance the learning of the pupils and to aid the staff in their delivery of the curriculum. This policy will set out a framework for how ICT/Computing will be used, taught, assessed and monitored safely and effectively throughout the school and reflects our ethos. It should be read in conjunction with other policies including Anti-Bullying, Behaviour, PSHE, Child Protection, Code of Conduct, Data Protection, Copyright Protection and Freedom of Information policies.

**Aims/Rationale**

ICT/COMPUTING encompasses every part of modern life and it is important that our children are taught how to use these tools safely. We believe that it is important for children, staff and the wider school community to have the confidence and ability to use these tools to prepare them for an ever-changing and rapidly developing world. To enable all our staff and pupils to be confident, competent independent users and learners of ICT/COMPUTING we aim:

- To use ICT/COMPUTING to motivate and inspire pupils and staff in all areas of the curriculum
- To use ICT/COMPUTING to help improve standards in all subjects across the curriculum
- To develop the ICT/Computing competence and skills of pupils through ICT/Computing lessons and provide them with the chance to consolidate these in a cross-curricular context
- To ensure pupils are challenged in their use of ICT/Computing and are provided with exciting, creative ways in which to share their learning and excel
- To use tools available to ensure children have the ability to work independently and collaboratively to suit the needs of the situation
- To provide all staff with the training and support to ensure that they can, and have the confidence to, use ICT/Computing safely to its full potential in all aspects of school life
- To use ICT/Computing as a form of communication with parents, pupils and the wider community
- To ensure that parents and pupils are fully aware of ways in which the internet and ICT/Computing can be used productively and safely.
- That before launching any system or initiative, we will make sure that the children's safety is at the forefront of our thoughts and we will keep parents informed as necessary through newsletters and parents events.
- To make available a range of e-safety information on the school website.
- We will conduct an annual survey of parents and pupils to ascertain internet use at home and publish results from this in the school newsletter and on our website.
- To promote children's involvement with the ICT/Computing curriculum through Digital Leaders

**Curriculum**

ICT/Computing will be taught and used across the curriculum. Stand-alone ICT/Computing sessions will teach skills that can then be applied in the cross-curricular sessions. Children may be taught ICT/Computing using the ICT suite or the computers and other equipment in classrooms. The ICT/Computing curriculum map will show the journey in which the children are expected to take but this will be reviewed each year to ensure that it is relevant and up-to-date. There will be a growing selection of age-appropriate ideas on the KAPS website.

The ICT Manager, working with the Senior Leadership/ Management Team, will ensure that the plans provide coverage of the National Curriculum Programmes of Study and that children are challenged and are able to succeed. In Nursery and Reception, children will be taught how to use various pieces of ICT equipment, including the computers, in accordance to the Early Learning Goals appropriate for them.

**1. Online Learning**

As a school, we value the importance of providing opportunities for children to learn outside of school and we will provide these depending on the age of the child.

On our website, for children in Foundation and Key Stage 1 we will:

- Provide links to generic websites suitable for the age phase (e.g. phonics)
- Provide links to websites suited to the current topic
- Provide logins for online tools such as Education City

For children in years 5 and-6, we will also:

- Provide a personal login for our class blogs
- Homework activities on Education City and Espresso Education

**2. Assessment**

Initially, ICT/Computing will be assessed using *Switched on Computing Assessments* which follows the recommendations of the DfE's National Curriculum Expert Panel relating all assessment to the content of the programme of study. Each unit includes a number of assessable outcomes, presented in the format 'all', 'most' and 'some', which are then mapped to corresponding statements from the programme of study.

At the end of each half term, tracker children will complete a self-evaluation form to evaluate their progress and learning of the ICT/Computing skills covered. Staff will also assess tracker children against a series of 'I can' statements that relate to the skills in the ICT curriculum map. Samples of tracker children's work will be saved on Teacher Share area of the network as evidence.

**3. Equal Opportunities and Inclusion**

We will ensure that all pupils are provided with opportunities to access the ICT/Computing curriculum throughout the school. Where necessary, we will endeavour to make adaptations to the environment or provide software that will enable all learners to achieve. We are aware that not all families may be able to access ICT equipment at home and we will address this on an individual

basis. Specific hardware and software can be used to address children's needs, for example Education City.

**4. Roles and Responsibilities**

**Roles and Responsibilities - Senior Management Team**

The head teacher, ICT Manager and the senior management team (SMT) are responsible for monitoring the teaching of ICT/Computing throughout the school. They will oversee the completion of the Self-Review Framework and E-Safety Framework. The SMT decide on the provision and allocation of resources throughout the school in accordance to the school improvement plan, ICT action plans and timescales. They should also ensure that the ICT Manager//ICT Network Manager and teachers are following their roles as listed below and in accordance to job specifications and performance management targets.

**Roles and Responsibilities - ICT Manager; SLT; SMT**

The ICT Manager/ICT Network Manager, in conjunction with SMT, will oversee planning in all year groups throughout the school and be responsible for raising standards in ICT. They are responsible for informing staff of new developments and initiatives and providing training where appropriate. They are responsible for keeping the hardware inventory up-to-date and ensuring the school has the appropriate number, and level, of software licenses for all software within the school. The ICT Manager/ICT network Manager and SLT are responsible for managing equipment and providing guidance for future purchasing. The ICT Manager/ICT Network Manager are also responsible for ensuring tools and procedures are sustainable.

**Roles and Responsibilities - Teachers**

All teachers, including student teachers have a responsibility to plan and teach ICT and to use ICT within their class. This will be in accordance to the Computing curriculum map provided by the ICT Manager. They will also assist in the monitoring and recording of pupil progress in ICT. Teachers should also respond to, and report, and e-safety or cyber bullying issues that they encounter within or out of school in accordance to e-safety procedures as listed below.

**Roles and responsibilities – Support staff**

Support staff may assist children in using ICT/Computing as planned for by the class teachers/ICT Manager or provide direct teaching. Support staff should also respond to, and report, any e-safety or cyber bullying issues that they encounter within or out of school in accordance to e-safety procedures as listed below. These will be taken into account when the ICT/Computing policy is next reviewed by the governing body.

**Roles and responsibilities – Digital Leaders (DLs)**

The Digital Leaders apply for the role in Year 5 and are selected based on an interview basis to provide a pupil voice regarding how ICT/Computing is taught and used within school as well as technical support for the ICT Manager. Their duties include running clubs, testing software and peer to peer support.

DLs should also respond to, and report, any e-safety or cyber bullying issues that they encounter within or out of school in accordance to e-safety procedures as listed below.

**Roles and Responsibilities - Governors and visitors**

The governing body will be emailed with the ICT/Computing policy and should review it at regular intervals to take into account any issues that have been reported by staff and/ or changes to practice, guidance and statutory duties that need to be made.

School governors should abide by the guidelines set out for staff and ensure that if they do use the computers and equipment within school that they are doing so safely. If either a visitor or governor wishes to have an account to logon to the school network, they should speak to a member of the senior management team.

**Roles and Responsibilities - Pupils**

Pupils will be taught how to use ICT/Computing resources and expertise across the curriculum and they will be able to apply these skills to their work. They will be able to engage with the curriculum through homework, blogs educational sites and opportunities are given to access the Internet given if children lack it outside school.

Pupils should follow the guidelines laid out in the AUP. They should ensure that they use the computers and equipment appropriately at all times.

It is expected that children will follow the school's behaviour policy when working online. They are also expected to adhere to the school's anti-bullying policy. If the children fail to do so, then the procedures outlined in these policies will come into force.

**Roles and Responsibilities – Parents**

Family learning is important to our school ethos and parents will be encouraged to access adult learning through use of ICT/Computing equipment on school premises. We will work with them to support their children's learning and to access information via the school's website where necessary.

Parents should stay vigilant to the websites and content that their children are accessing on computers and other devices like mobile phones. They should also try to talk to their child about e-safety and the use of the internet. If they have any questions or concerns then they should speak to their child's teacher, the ICT/Network Manager or the head teacher.

**5. Hardware and Software**

KAPS is committed to ensuring that ICT/Computing skills underpin pupils' learning across the whole curriculum and to do this we are committed to keeping all equipment up to date and in good working order. This means that we have upgrades of hardware and software included in our forward planning. The ICT Manager/Network Manager and SMT will keep themselves up to date with technological updates as they impact on learning at home and school.

Installation of software, management of hardware and the Network is the responsibility of the ICT Manager and the Network Manager and will be done abiding by contractual requirements linked to licences.

Back to top

Hardware should not be installed without the permission of the head teacher and/or ICT/Network Manager. If staff use memory sticks then the school's antivirus software will scan these. Staff should be vigilant to reduce the risks of virus infection as stated in the AUP.

The installation of software unauthorised by the school, whether licensed or not, is forbidden. If you are unsure, please speak to the head teacher and/or the ICT/Network Manager for advice. The school reserves the right to examine or delete any files that are held on its system.

We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected data has been used or held, and get a certificate of secure deletion for any server that once contained personal data.

Staff are not permitted to take school laptops home. The settings on them are such that user accounts can only be accessed when they are connected to the school network. We use encrypted flash drives if any member of staff has to take any sensitive information off site.

Any staff member who borrows ICT equipment will fill in a loan agreement form. This form assigns primary responsibility of the devices listed to the borrower. When signing out devices, staff accept responsibility for the safe handling, due care and safe return of the equipment as per the schools Acceptable Use Policy. If it is determined that the loss or damage of the equipment is a result of negligence, the borrower may be held financially responsible for the repair or replacement of the equipment.

**6. Network**

Staff will be issued with a username for the computer consisting of their first initial and surname and a password. It is their responsibility to change this in accordance with the password procedure below. The network will prompt users to change their passwords at regular intervals to ensure security. These passwords are unique to the staff member and it is a breach of the Data Protection Act to reveal it or give access to a 3rd person. Staff should keep passwords in a safe place and not displayed for others to see.

Students and visitors are granted access to the network on a temporary basis and will need to speak with the ICT/Network Manager to get this. They will be asked to sign the Acceptable User Agreement and undergo induction linked to safeguarding and E-Safety. Pupils are issued with individual logins that consist of their first initial and surname and a password of 'password1.' This cannot be changed.

**7. Backups**

The data stored on the school's network is scheduled to back up on-a daily basis.. This will allow backups of files to be recovered if the original becomes lost or damaged.

**8. School Website and Blogs - Linked to 360Safe Public Facing and Professional Standards Guidelines**

The school website will be overseen by the ICT Manager and it is expected that certain pages may be updated by other members of staff and children.

**9. E- safety**

**Internet and E-mail**

The internet may be accessed by staff and by children throughout their hours in school. We ask as a school that staff are vigilant as to the sites children are accessing and children should not be using the internet unattended.

The teaching of internet use will be covered within the Computing curriculum planning, but staff should encourage regular dialogue that explores the benefits and potential dangers of using the internet.

All members of staff will be issued with a school email address and this is the email with which they should use for professional communication. Personal email accounts are not to be used and if this is breached the employee may be subject to disciplinary procedures. Users are responsible for all messages that are sent and due regard should be paid to the content of the emails to ensure it is not misconstrued. All web activity is monitored by the ICT/Network Manager so it is the user's responsibility to ensure they log off appropriately.

The use of the internet to access inappropriate materials such as auction sites, pornography, racist or any other material is prohibited. If users, especially children, do see an inappropriate website or image, they should close this immediately and report the site to their class teacher who should inform the ICT/Network Manager.

The internet and filtering is provided by the local authority. Inappropriate websites are filtered out by the local authority.

Whilst checking of personal sites, e.g. email, is permitted during break times, staff should be aware that this should only happen for a brief time and that they should be extra vigilant and ensure they are logged off appropriately. Staff follow, and agree to, the Acceptable Usage Policy.

**10. Passwords – Linked to 360Safe Password Guidelines**

For online services used in school such as our blogs, there is an account per class and staff will be given a password that matches their unified sign on (USO) password issued by LGfL. This password will also access LGfL email and other tools provided by them like PurpleMash.com.

Children have another username and password for Education City that is issued by Education City.

Staff can change their blog passwords, but should make sure that any passwords they use are strong and contain a mixture of some of the following; upper- and lower-case letters and numbers. These should be changed regularly, especially if the user suspects others may know the password.

**11. School Liaison, Transfer and Transition**

When a new child joins, it is the responsibility of office staff to inform the ICT/Network Manager of the child's name and year group. The ICT/Network Manager will then provide a network login and provide accounts for the online tools available.

As part of the admissions process permission to take photos of children to use in school and on the website will be sought, this is then recorded on SIMs. Families are also made aware of the Data Protection Act and its place within school. School staff with access to SIMs will check to ensure photos are only taken where permission has been given.

Once they have left our school, the child's account will be removed from the online tools and their content will be removed by the ICT/Network manager.

**12. Mobile phones**

SMART phones are mini computers and as such are open to misuse to keep adults and pupils safe we do not allow mobile phones on in classrooms or any area that children are working. This is key to safer working practices and inappropriate use will lead to disciplinary procedures.

Mobile phones should be off and locked away during school time. They can be checked at break and lunch times. Staff members should never use their mobile phones to capture images or children. Personal telephone numbers MUST not be shared with children or parents. In the unlikely instance that a personal phone is used to contact a parent the number must be blocked.

School mobile phones are available to SLT who have a responsibility for safeguarding and may need to call in case of emergency e.g. child has left the site. Phones are also allocated to the ICT Manager; caretaking staff and Children's centre staff as a key part of their role. A school mobile is available for the lead professional to take on class trips for emergency use.

We acknowledge that in emergencies staff may need to be contacted urgently and in this instance permission must be sought from the SLT to keep the phone on silent. It must not be used where children are present.

**13. Age Limits**

Certain online tools have age limits on the use of their software. This is due to an Act of United States Law. The Children's Online Privacy Protection Act prevents websites collecting data or providing their services to users under the age of 13.

As a school, we may decide to use some of these tools within lessons but will do so after thoroughly testing them for their safety and appropriateness. We will also post details of these sites on our school webpage. We will ensure that these will tend to be sites that allow creation of content rather than searching other users' content.

Occasionally these sites will be used by teachers with a class, for example to create a class book or movie, but not by a child with their own personal account. We will make parents aware of this during our e-safety events. If they do not wish their child to access these sites, their child can be provided with an alternative method to complete the task.

**14. Personal Data**

Staff should be aware that they should not transfer any protect or restricted material items that contain personal data such as reports and contact information on to personal devices unless it is encrypted and strictly necessary.. This data should then be removed as soon as possible. When using a laptop or device containing student data, staff should be extra vigilant to not leave this device lying

around or on display. Where a user finds a logged-on machine, we require them to always log-off and then log on as themselves. Users needing access to secure data are timed out after 15 minutes and have to re-enter their username and password to log back on to the network. This is enforced automatically through software configuration. The school assessment package, School Pupil Tracker (SPTO) is an online site and gives users access to student data. Users are required to follow e- safety guidelines to ensure this information cannot be accessed by a 3rd party and to sign the acceptable user policy (AUP).

**15. Social Media**

**Definition of social media**

- For the purposes of this policy, social media is a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes online social forums such as Twitter, Facebook and LinkedIn. Social media also covers blogs and video- and image-sharing websites such as YouTube and Flickr.
- Employees should be aware that there are many more examples of social media than can be listed here and this is a constantly changing area. Employees should follow these guidelines in relation to any social media that they use.

**Use of social media at work**

- Employees should not spend any time while at work using social media websites. They should ensure that use of social media does not interfere with their duties and use of social media does not have a detrimental effect on their productivity.
- Employees are allowed to access social media websites from the school's computers or devices at certain times (provided that they are not undertaking overtime). Employees must limit their use of social media to their official break times such as their lunch break and before and after their normal working hours (unless it is a genuine requirement of the employee's job).
- The School understands that employees may wish to use their own computers or devices, such as laptops, palm-top and hand-held devices, to access social media websites while they are at work. Employees must limit their use of social media on their own equipment to their official break times, such as their lunch break.

**Monitoring use of social media during work time**

- The School reserves the right to monitor employees' internet usage, but will endeavour to inform affected employees when this is to happen and the reasons for it. The School considers that valid reasons for checking employees' internet usage include suspicions that employees have:
    - been using social media websites when he/she should be working; or
    - acted in a way that is in breach of the rules set out in this policy.
    - The School reserves the right to retain information that it has gathered on employees' use of the internet.
    - Access to particular social media websites may be withdrawn in any case of misuse.

**Social media in your personal life**

- The School recognises that many employees make use of social media in a personal capacity. While they are not acting on behalf of the School, employees must be aware that they can damage the reputation of the organisation if they are recognised as being one of our employees.

- Even if an employee does not specifically name the School on social media, it is likely that some viewers will know who they are employed by and as such communications still have the potential to bring the organisation into disrepute.
- Employees are allowed to say that they work for the School, which recognises that it is natural for its staff to sometimes want to discuss their work on social media. However, the employee's online profile (for example, the name of a blog or a Twitter name) must not contain the School's name.
- If employees do discuss their work on social media (for example, giving opinions on their specialism or the education sector), they must include on their profile a statement along the following lines: "The views I express here are mine alone and do not necessarily reflect the views of my employer."
- Any communications that employees make in a personal capacity through social media must not:
    - have the potential to bring the School into disrepute, for example:
        - by criticising or arguing with parents, colleagues or rivals;
        - by making defamatory comments about individuals or other organisations or groups; or
        - by posting images that are inappropriate or links to inappropriate content;
    - breach confidentiality, for example:
        - by giving away confidential information about an individual (such as a colleague or pupils) or the School; or
        - by discussing the School's internal workings (such as future plans that have not been communicated to the public, parents or pupils);
    - breach copyright, for example:
        - by using someone else's images or written content without permission;
        - by failing to give acknowledgement where permission has been given to reproduce something; or
    - do anything that could be considered discriminatory, bullying or harassment of an individual or group, for example:
        - by making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
        - by using social media to bully or criticise another individual (such as an employee of the organisation); or
        - by posting images that are discriminatory or offensive, or links to such content.

**Disciplinary action over social media misuse**

- Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against the employee and/or the School. It may also cause embarrassment to the School.

- In particular uploading, posting, forwarding or posting a link to any of the following types of material on a social media website or via email, whether in a professional or personal capacity, will amount to gross misconduct:

    - pornographic material;
    - a false or defamatory statement about any person or organisation;
    - material which is potentially offensive, obscene, discriminatory, derogatory or may cause embarrassment to the School, or its staff;
    - online bullying of colleagues;
    - social media activity with the potential to cause damage to the reputation of the organisation;
    - confidential information about the School, any of our staff or pupils (for which there is no express authority to disseminate);
    - any other statement which is likely to create any liability (criminal or civil);
    - material which breaches copyright or other intellectual property rights, or which invades the privacy of any person.

    Any such action will be addressed under the Schools Disciplinary Procedure and is likely to result in summary dismissal.

- Where evidence of misuse is found the School may undertake a more detailed investigation in accordance with its Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the investigation. If necessary such information may be handed to the police in connection with a criminal investigation.

- Any use of social media by other members of staff in breach of this policy must be reported to the Head teacher.

These are safer working practices and inappropriate use of social networks will lead to disciplinary procedures. Staff follow, and agree to, the Social Media Acceptable Usage Policy at the end of this document.

**Pupils:**

Pupils should not be signed up to most social networking sites due to the over-13 age limit. However, we recognise that many are signed up either with or without parental knowledge therefore as a school we will:

- Monitor the use of social networking and ensure it is part of our curriculum.

- We will also ensure that parents are fully aware of how to minimise the risk if their children are using these sites.

- We reserve the right to contact sites such as Facebook and ask them to remove our children's accounts should any issues, such as cyber-bullying, occur.

- Use blogging throughout the school to share children's learning and to communicate with parents. We will follow guidance laid out in this document to ensure children are kept safe.

No-one is able to post on the blog or write a comment without it being approved by a teacher to ensure that the children are not subjected to any inappropriate comments.

- Monitor spam messages (often containing inappropriate links and language) are caught by software installed on the system and this is monitored by the ICT/Network Manager. This is also updated regularly.

- Ask parents and pupils about their use of social media to ascertain the number using sites such as Facebook.

**16. Digital and Video Images - Linked to 360Safe Digital and Video Guidelines**

At no time should staff use personal devices, such as cameras or mobile phones, to capture images of children. Personal devices such as these should be locked away during school time.

Images of children should only be processed on school computers and not saved on personal devices, including USB sticks. Photos of children should be saved in the designated area of Teacher Share.

Staff should only photograph and video children at appropriate times and for legitimate reasons such as during lesson times or as part of a club. Staff should never be alone with an individual child when photographing or recording.

Failure to follow these procedures will result in disciplinary action being undertaken.

As a school we will ensure that if we publish any photographs or videos of children online, we:

- Will have asked parents or carers for permission first when children are admitted into the school
- Will ensure if we do not have permission to use the image of a particular child, we will make them unrecognisable to ensure that they are not left out of situations unnecessarily
- Will not include a child's image and their name together without permission from the parents or guardians e.g. if the child has won an award
- Will ensure that children are in appropriate dress and we do not include images of children who are taking part in swimming activities
- Ask that if a parent, guardian or child wishes, they can request that a photograph is removed. This request can be made verbally or in writing to the child's teacher or to the ICT Manager. We will endeavour to remove the photograph as soon as possible
- Will provide new parents with a photo permission letter upon their arrival into school
- Will ask parents or guardians that are recording video or taking digital images at public events e.g. school play or sports day, that they do not publish these online

**17. Technical Support**

Many minor issues are dealt with by the ICT/Network Manager and the Digital Leaders as appropriate.
Hardware technical support is provided by the ICT/Network Manager when required.

Additional office-based support (e.g. MIS, SIMs) is provided by Octavo Partnership Limited and forms part of the annual Service Level Agreement that the school has in place.

**18. Sustainability and Environmental Impact – Linked to ICT Mark 1b4**

To ensure that the level of ICT across the school is sustainable, the ICT/Network Manager is responsible for the upkeep of usernames, passwords and software as well as details of licenses and a complete ICT Inventory.

Hardware is disposed of safely and securely.

**19. E-Safety – Linked to 360Safe E-Safety Guidelines**

We take e-safety very seriously at KAPS and KACC. We will ensure that it is taught often throughout the children's Computing sessions as necessary. We will also provide children with dedicated e-safety lessons per term. All e-safety lesson plans and resources will be available on the school website for parents to view. These will be reviewed regularly to ensure that they are up-to-date and reflect current needs. Children will be taught how to act online and how to minimise the risk when working on the internet. Pupils will also be taught about managing passwords, respecting copyright and other elements of this policy that are relevant to them. Tracker children will take part in e-safety audits before and after the designated lessons in order to monitor impact.

Our plans will provide children with an understanding of the expectations we have of them at a level appropriate to their age. We will also have an annual e-safety focussed parent meeting and will provide regular updates via our website and newsletters as appropriate.

All children will be taught about the Acceptable Use Policy and will sign a copy related to their age phase. These will be stored by the ICT Manager. All staff will also complete an AUP. Useful ICT rules will also be posted in the ICT suite and near classroom computers to ensure they are seen by children and visitors.

E-safety training will also be provided for staff and governors to ensure that they conduct themselves in the appropriate manner when working and communicating online. The ICT Manager will also carry out e-safety staff audits before and after training to monitor its impact. All new staff will be subject to e-safety audits and training.

If there is a website available to children that staff or children deem inappropriate they can either complete the online form or speak to the ICT/Network Manager who will then contact Croydon LA to attempt to get this blocked.

If a teacher suspects an e-safety issue within school they should make notes related to the incident in accordance to anti-bullying and behaviour policies. This should then be reported to the ICT Manager and head teacher and recorded as appropriate.

If children receive an email, text message or similar that they believe to be inappropriate then they should leave it (not delete it) and inform their parents/carers, their teacher and/or the ICT Manager who will investigate.

On all school blogs children will be provided with a button/page to report a problem to the ICT Manager should they find something inappropriate.

**20. Complaints**

Incidents regarding the misuse of the Internet by pupils will be delegated to the ICT Manager, in liaison with SLT, who will decide which additional evidence should be gathered or recorded. A partnership approach with parents will be encouraged. Any complaint about staff misuse will be referred to the head teacher in writing. Complaints of a child protection nature must be dealt with in accordance with child protection procedures.

**21. Copyright and Intellectual Property Right (IPR)**

Copyright of materials should be respected. This includes when downloading material and/or copying from printed materials. Staff should not remove logos or trademarks unless the terms of the website allow it.

Staff should check permission rights before using materials, particularly images, from the internet. Children will be taught in Key Stage 2 to begin to consider the use of images from the internet. In year 3/4 they will have discussions about the proper use of images with questions such as 'Is it OK to use an image we find online?' As they progress to year 5/6 some children should start referencing the sites they have used. This could be as simple as putting the name of the site the image came from or a hyperlink. It is not expected for children to include a full reference but to be *aware* that it is not acceptable to take images directly from the internet without some thought on their use.

**22. Responding to Unacceptable Use**

**Responding to unacceptable use by staff**

Failure to comply with the guidelines and expectations set out for them could lead to sanctions being imposed on staff and possible disciplinary action being taken in accordance with the school's policy and possibly the law.

**Responding to unacceptable use by pupils**

Pupils should be aware that all e-safety issues will be dealt with quickly and effectively. When dealing with unacceptable use, staff should follow the behaviour policy and if necessary, the anti-bullying policy. Children may have restrictions placed on their account for a short time.

**23. Acceptable Usage Policy Guidelines**

**Acceptable Usage Policy Guidelines – Staff (Linked to 360Safe AUP Guidelines)**

This document has been written to ensure that staff use the ICT throughout the school appropriately and refers to the detail contained in our E- safety Policy. Any questions regarding this policy should be directed to Senior Management team or the ICT Manager.

**Staff should:**

- Ensure that they have read and understood the ICT/Computing and E- Safety Policies
- Use computers and equipment with care and ensure children do the same e.g. water bottles should stay away from machines
- Ensure that they have strong and secure passwords
- Ensure that usernames and passwords are not shared with children or other staff and software packages, such as SIMS and LGFL staff mail should not be left opened when the computer is unattended.
- Ensure that they log off when they have finished using a computer or any software package
- Make use of resources such as cameras and microphones but ensure that these are returned after their use. They should also endeavour to remove pictures/files on return too
- Try not to be wasteful, in particular when it comes to batteries, printer ink and paper
- Ensure that online dialogue (e.g. blog posts or emails) with other schools, parents or children remains professional at all times
- Ensure that online activity is related to their professional duty and that personal use should be kept to a minimum
- Ensure that they are not using the school's ICT for financial gain e.g. auction or betting sites, frequently printing non-work related materials
- Be aware that software or hardware should not be installed without prior consent of the ICT/Network Manager or head teacher
- Understand that inappropriate use of the school's network may result in some services being removed and further action being taken by the head teacher
- Ensure data of a personal nature such as school reports, IEPs, correspondence, photographs and assessment data is not taken home on a personal storage device unless strictly necessary and done so using an encrypted device. It must be recognised that this data comes under the Data Protection Act and is subject to the school's Data Protection Policy. Care must therefore be taken to ensure its integrity and security. It must not be transferred to home computers and should be removed from any portable device including encrypted USB pens and memory cards as soon as is practical.
- Report any issues to the Senior Management team or ICT/Network Manager as soon as possible where any equipment has gone missing e.g. staff tags, SD cards, camera chargers or batteries etc.
- Return any hardware or equipment if they are no longer employed by the school.

**Acceptable Usage Policy Guidelines - KS2 Children (Linked to 360Safe AUP Guidelines)**

This document is to provide some guidelines to ensure that you stay safe and act responsibly when using the computers and refers to the detail contained in our E- safety Policy. . When we talk about ICT/Computing, we are talking about computers, laptops, and everything else including cameras, USB microphones and other devices. By using the ICT/Computing in school, you have agreed to follow these rules. These rules will be discussed with you as a class before you sign them. A copy of this will also be sent home to your parents.

If you have any questions, please ask your teacher or the ICT/Network Manager.

- At all times, I will think before I click (especially when deleting or printing)
- When using the internet, I will think about the websites I am accessing
- If I find a website or image that is inappropriate, I will tell my teacher straight away
- When using information or pictures from websites, I will try and say which website it came from and if possible link back to the site
- When communicating online (e.g. in blogs) I will think about the words that I use and will not use words that may offend other people
- When communicating online, I will only use my first name and not share personal details such as my email address or phone number
- I understand that people online might not be who they say they are
- I will not look at other people's files or documents without their permission
- I will not logon using another person's account without their permission
- I will think before deleting files
- I will think before I print
- I know that the teachers can, and will, check the files and websites I have used
- I will take care when using the computers and transporting equipment around
- I will keep my usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents or teachers
- I will log off a computer when I am finished
- I will not install any software or hardware (including memory sticks) without permission from a teacher
- I understand that if I am acting inappropriately then my parents may be informed

---

**Recommended Films for Children**

Be Safe e-Safe (Kent Police Video about Internet Safety)
Cyberbullying video (Digizen from Childnet)
CEOP Centre Corporate Film (Video to describe what CEOP does)
Where's Klaus (CEOP Clip about Internet Safety)
Jigsaw (CEOP video aimed at raising awareness about what constitutes personal information)

**Acceptable Usage Policy Guidelines KS1 Children (Linked to 360Safe AUP Guidelines)**

These rules have been written to make sure that you stay safe when using the computers. This includes cameras and microphones too. By using the ICT in school, you have agreed to follow these rules. Your teacher will talk about these rules before you sign them and a copy will be sent home to your parents.

If you have any questions, please ask your teacher or Nadia.

The Golden Rule: **Think before you click**

☺ I will be careful when going on the internet.

☺ I will only use the internet when a teacher is with me.

☺ I will tell a teacher if I see something that upsets me.

☺ I know people online might not be who they say they are.

☺ I will be polite when talking to people or writing online.

☺ I will think before I print or delete.

☺ I will be careful when using or carrying equipment.

☺ I will keep my password secret, but I can tell my family.

☺ I will remember to log off properly when I am finished on a computer.

☹ I won't tell anyone any personal details like my phone number or last name.

☹ I won't logon using someone else's username.

☹ Never put water bottles on the table when using ICT.

---

**Recommended Films for Children**

Be Safe e-Safe (Kent Police Video about Internet Safety)
Cyberbullying video (Digizen from Childnet)
CEOP Centre Corporate Film (Video to describe what CEOP does)
Where's Klaus (CEOP Clip about Internet Safety)

**E-Safety Policy (Including Digital Images and Networking)**

**For Kensington Avenue Primary School (KAPS) and Children's Centre (KACC)**

The use of cameras should be considered an essential and integral part of everyday life. As such, children, young people and staff are to be encouraged to use such technology in a positive and responsible way.

It has to be recognised however, that digital technology has increased the potential for cameras and images to be misused and inevitably there will be concerns about the risks to which children and young people may be exposed.

We recognise that having the right policies and practices in place will also protect school staff from misunderstanding, false accusations and damage to reputation around the use of digital images.

Practical steps must be taken to ensure that the use of cameras and images will be managed sensitively and respectfully. A proactive and protective ethos is to be reflected which will aim to promote effective safeguarding practice.

It must, however, be acknowledged that technology itself will not present the greatest risks, but the behaviours of individuals using such equipment will.

The Camera and Image Policy will aim to ensure safer and appropriate use of cameras and images through agreed acceptable use procedures. This is to be in line with legislative requirements and will aim to respect the rights of all individuals.

The Camera and Image Policy will apply to all individuals who are to have access to and/or be users of work-related photographic equipment. This will include children and young people, parents and carers, early year's practitioners and their managers, volunteers, students, committee members, visitors, contractors and community users. This list is not to be considered exhaustive.

The Camera and Image Policy will apply to the use of any photographic equipment. This will include mobile phones, tablets, video cameras, webcams and portable gaming devices with inbuilt cameras as well as other forms of digital technology and resources for storing and printing images.

The Senior Designated Professional for Safeguarding is to be responsible for ensuring the acceptable, safe use and storage of all camera technology and images. This will include the management, implementation, monitoring and review of the Camera and Image Policy.

This policy complies with the requirements of the Data Protection Act 1998, Freedom of Information Act 2000, Human Rights Act 1998 and other relevant Acts regarding the taking and use of photographic images of children.

All images will be used in a manner respectful of the eight Data Protection Principles. This means that images will be:

- **i.** Fairly and lawfully processed
- **ii.** Processed for limited, specifically stated purposes only
- **iii.** Used in a way that is adequate, relevant and not excessive
- **iv.** Accurate and up to date

**v.** Kept on file for no longer than is necessary
**vi.** Processed in line with an individual's legal rights
**vii.** Kept securely
**viii.** Adequately protected if transferred to other countries.

Where necessary, registration as a data controller will be applied for to allow personal information to be processed.

**At <u>Kensington Avenue Primary School and Children's Centre</u> all staff, parents / carers and, where age appropriate, pupils are required to sign the appropriate Acceptable Use Policy. When taken together these cover the requirements of, and set out the procedures for, the taking and storage of photographs, digital images and videos. Additionally, all parents are asked to sign to give their consent to photographs, digital images and videos being taken and are made aware of the contexts, nature and the use to which these will be put when their children join the school/ Children's Centre.**

**The relevant Acceptable Use Policies are contained in Appendices 1, 2 and 3 of this document.**

**Appendix 1**

- Staff using ICT/Computing at KAPS and KACC
- Use of School Mobile Phones
- Use of Staff iPads at KAPS and KACC
- Supply Teachers and Visitors Agreement Form

**Appendix-2**

- E-safety Agreement Form: Parents KAPS and KACC
- Use of Digital and Video Images Policy
- The use of Digital Image and Video
- The use of Social Networking and On-line Media

**Appendix-3**

- Key Stage 2 Children
- Key Stage 1 Children

**Ratified by……**

**Date……**

**Review date……**

**Appendix 1**

| | | |
|---|---|---|
| | **Kensington Avenue Primary School (KAPS) and Kensington Avenue Children's Centre (KACC)** | |
| | **AUP review Date** | **October 2017** |
| | **Date of next Review** | **October 2018** |
| | **Name** | |

**Acceptable Use Policy (AUP):**
**All Staff, Volunteers and Governors using ICT/Computing at KAPS and KACC**

This covers use of digital technologies in **KAPS and KACC**: including email, Internet, intranet and network resources**,** learning platform, software, equipment including mobile phones, tablets, e-readers and systems.

- I acknowledge and accept that personal mobile and electronic devices (including but not limited to laptops, tablets and mobile phones) must not be connected to the schools wireless network
- I will only use the Kensington Avenue Primary School and Children's Centre's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Senior Leadership Team.
- I accept and will follow the school's policy on use of mobile phones and other electronic devices at school as per the schools Acceptable Use Policy. I acknowledge and accept that such devices must never be taken into or used in classrooms or pupil learning environments. Personal electronic devices can only be used in the staffroom
- I will not bring on to the school premises or use personal mobile devices and/or electronic devices without gaining the approval of the schools ICT department.
- I understand any personal mobile and/or electronic device brought in must be shown to the ICT department where it will be inspected. The device must be signed in on each occasion before use on-site is permitted. Where permission has been denied, the device must not be used anywhere on the premises.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not reveal my password(s) to anyone including other members of staff/supply cover.
- I will not display my passwords and login details in public sight or leave them where others can find. This includes sticky labels on laptops or cupboard doors
- I will not allow unauthorised individuals to access any of KAPS and KACC systems.
- If I use Student Pupil Tracker Online (SPTO) off school premises to enter in children's assessments; I will ensure that all 3rd party individuals cannot access any personal data of the children.

- I will ensure all documents, data, information etc., are saved, accessed and deleted in accordance with the KAPS and KACC network and confidentiality protocols.
- I will not compromise the security of the school network by leaving any device unlocked and unattended. Devices must be locked when not attended or logged off after use.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I understand that any / my personal online communication tools must not be used with children's families and I will not communicate or 'befriend' any children and/or families using such methods.
- I will only use the approved email system for any email communication related to work at Kensington Avenue Primary School and Children's Centre This is currently: LGFL staff mail
- I will only use other KAPS and KACC approved communication systems for any communication with young people or parents/carers. In this organisation the systems used are: LGFL staff mail, Call Parent, the school website and KAPS Blog.
- I will not browse, download or send material that could be considered offensive to colleagues or of an extremist nature.
- I will not support or promote extremist organisations, messages or individuals
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / KAPS and KACC named contact. This is: Nadia Da Silveira / Dean Dumont.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the Kensington Avenue Primary School and Children's Centre's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of young people or staff without permission from SLT and will not store images at home without permission.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role. I understand that it is my responsibility to ensure I know how to use any such tools so as not to compromise my professional role, such as setting appropriate security settings.
- I will not create a business account on any social networking site unless in full agreement with the appropriate manager, agreed for specific circumstances.
- I agree and accept that any computer, laptop, mobile phone or tablet loaned to me by KAPS and KACC is provided solely to support my professional responsibilities and that I will notify them of any "significant personal use" as defined by HM Revenue & Customs.
- I will access KAPS and KACC resources remotely (such as from home) only through approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow KAPS and KACC data security protocols when using any such data at any location.

- I understand that data protection policy requires that any information seen by me with regard to service users, held within the KAPS and KACC LA's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I agree to sign a loan agreement form for all equipment loaned to me and accept the terms and conditions as per the schools Acceptable Use Policy.
- I will make sure that if any equipment and/or accessories (e.g. laptops, iPads, staff tags, and camera leads/chargers) are misplaced, lost or stolen; I will report it to the ICT Manager/Network Manager or member of the SLT.
- I accept that equipment loaned to me is my responsibility and there may be costs at my own expense applicable to repair or replace any equipment and/or accessories lost or stolen whilst in my possession due to exposure to a non-insured risk and/or failure to undertake proper care.
- I will ensure that KAPS and KACC equipment is stored in a safe place and all teacher laptops, iPads and cameras are locked away at the end of each day.
- I understand that it is my duty to support a whole organisation safeguarding approach and I will alert the KAPS and KACC named child protection officer / relevant senior member of staff if I feel the behaviour of any service user or member of staff may be a cause for concern or inappropriate.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request. I understand that failure to comply with this agreement could lead to disciplinary action.

**I agree to abide by all the points above.**

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the Kensington Avenue Primary School and Children's Centre's most recent e-safety policies.

Signature .....Date.....

Full Name ..... ..... (Printed)

Job title .....

KAPS □ KACC □ (please tick)

**Authorised Signature**

I approve this user to be set-up.

Signature ..... Date .....

Full Name ..... (printed)

| | | |
|---|---|---|
| | **Kensington Avenue Primary School (KAPS) and Kensington Avenue Children's Centre (KACC)** | |
| | **Policy review Date** | **October 2017** |
| | **Date of next Review** | **October 2018** |
| | **Name** | |

**Acceptable Use Policy (AUP):**
**Use of School Mobile Phones**

Staff provided with a school mobile purchased by the school, agree to the following terms of use:

- School mobile phones are issued strictly for work-related activities. Occasional personal calls of short duration may be necessary when no other immediate means of communication is available. Personal calls, incoming and outgoing, must be kept to a minimum and must be incidental to business use.
- The school reserves the right to cancel the mobile for abuse of phone privileges and/or department budgetary constraints.
- You are expected to protect the mobile phone from loss, damage or theft. If it is lost, stolen or damaged, the Head Teacher must be informed immediately
- Upon resignation or termination of employment, or at any time upon request, you must return the phone.
- No personal photographs should be taken on the school mobile phone.
- Do not store or leave unattended in vehicles.
- Phone records may be audited for compliance.

Please read and sign below:

I have read, understand and agree to abide by the terms of the **Mobile Acceptable Use Policy.**

Signature..... Date.....

Full Name..... (printed)

Job title.....

KAPS ☐ KACC ☐ (please tick)

| | Kensington Avenue Primary School (KAPS) and Kensington Avenue Children's Centre (KACC) | |
|---|---|---|
| | **Policy review Date** | **October 2017** |
| | **Date of next Review** | **October 2018** |
| | **Name** | |

**Acceptable Use Policy (AUP):**
**Use of Staff iPads at KAPS and KACC**

KAPS provides Apple iPads for staff to enable them to carry out their job role more effectively. This iPad remains the property of KAPS and is loaned to you for use within your job role.

- I accept and understand the iPad is my sole responsibility and must remain in my possession.
- I accept and agree that the iPad issued to me should only be used by me and should be securely stored when not in use.
- The iPad must not be taken off site unless permitted and a loan agreement form permitting this has been signed
- All iPad use must fully comply with the KAPS e-Safety Policy and Data Protection Policy. Failure to do so may lead to disciplinary action.
- The iPad may be connected to your school email account and might have access to personal pupil information. The iPad might also be used to store personal information such as picture and video images of pupils. This means you must fully comply with high standards of data protection.
- This iPad may be configured with certain restrictions in place. You must not try to make changes to the devices that are passcode protected.
- Loss or damage of the device should be reported to the Head teacher/ICT Manager immediately. If necessary the device will be remotely locked or wiped.
- Insurance cover provides protection from the standard risks whilst the iPad is on the school site or in your home **but excludes** theft from your car or from other establishments. Should you leave the iPad unattended and it is stolen or damaged, you will be responsible for its

replacement or repair costs and may need to claim this from your own insurance company if applicable.

- The iPad will be used in the classroom for teaching and learning. Remember that personal information might be accessible on the device and you must fully comply with high standards of data protection, therefore supervision of pupil use is required.
- *Any connection cost incurred by accessing the internet from outside school, other than through school-provided 3G, is not chargeable to the school.*
- This iPad may be recalled at any time checked for safety and for compliance with school policies. Outcomes will be reported to the Head teacher.
- If you leave the employment of the school the iPad must be returned in good condition to the ICT Network Manager before your official leaving date.

I have read and agree to the terms and conditions of this agreement and fully understand that I need to adhere to all elements.

iPad Model_____ Serial No._____ Asset ID_____

Signature..... Date.....

Full Name..... (printed)

Job title.....

KAPS ☐ KACC ☐ (please tick)

| | Kensington Avenue Primary School (KAPS) and Kensington Avenue Children's Centre (KACC) | |
|---|---|---|
| | **Policy review Date** | **October 2017** |
| | **Date of next Review** | **October 2018** |
| | **Name** | |

**Acceptable Use Policy (AUP):**
**Use of Social Media at KAPS**

As a school we fully recognise that social media and networking are playing an increasing role within every-day life and that many staff are users of tools such as Facebook, Twitter and blogs using these for both personal and professional use. We will ensure that staff and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks. All staff at KAPS have a responsibility to ensure that they protect the reputation of the school, and to treat colleagues and members of the school with professionalism and respect.

**Staff:**

- Should not accept current or ex-pupils as 'friends' on any social media sites such as Facebook. This is to ensure any possible misinterpretation. We do understand that some staff members have friends within the local community and just ask that these members of staff take extra precaution when posting online
- Must not use any form of social media to discuss any children or confidential KAPS information
- Must immediately report any inappropriate communications involving any child on any form social media
- Are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts. This also includes personal information such as phone numbers, email addresses etc.
- Should not use personal email accounts or mobile phones to make contact with members of the school community on school business, nor should any such contact be accepted, except in circumstances given prior approval by the Head teacher.
- Are aware of the potential off on-line identity fraud and to be cautious when giving out personal information about themselves which may compromise their personal safety and security.
- Should check with the ICT Manager/Network Manager if they need advice on monitoring their online persona and checking their security settings

| | | |
|---|---|---|
| | **Kensington Avenue Primary School (KAPS) and Kensington Avenue Children's Centre (KACC)** | |
| | **Policy review Date** | **October 2017** |
| | **Date of next Review** | **October 2018** |
| | **Name** | |

**Acceptable Use Policy (AUP):**
**Supply Teachers and Visitors Agreement Form**

- I will not use personal digital cameras or camera phones for taking and transferring images of any children or staff without permission from Senior Leadership Team and will not store images at home without permission.
- I will take responsibility when using any of the schools technologies, making sure that I use them safely, responsibly and legally.
- I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will respect copyright and intellectual property rights.
- I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
- I will not install any hardware or software onto the school system.
- I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

**User Signature**

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.
I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the Kensington Avenue Primary School and Children's Centre's most recent ICT/Computing policy (found on our website).

Signature..... Date.....

Full Name..... (printed)

Job title.....

KAPS ☐ KACC ☐ (please tick)

**Appendix 2**

| | | |
|---|---|---|
| | **Kensington Avenue Primary School (KAPS) and Kensington Avenue Children's Centre (KACC)** | |
| | **AUP review Date** | **October 2017** |
| | **Date of next Review** | **October 2018** |
| | **Policy reviewed by** | |

**Acceptable Use Policy (AUP):**

**E-safety agreement form: Parents of KAPS and KACC**

**Internet and ICT:** As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my child access to:

- the Internet at school
- the school's chosen email system
- ICT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.

**Use of digital images, photography and video:** I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

I will not take and then share online, photographs of other children (or staff) at school events without permission.

**Social networking and media sites:** I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.

Parent / Guardian name: _____

Pupil name(s): _____Class(s) _____

**Use of Digital and Video Images Policy**

**For Kensington Avenue Primary School (KAPS) and Children's Centre (KACC)**

**In our school:**

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the KAPS or KACC;
- Digital images /video of pupils are stored in a private teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's **Acceptable Use Policy** and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their eSafety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

**Website:**

- The Head teacher takes overall editorial responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers: ICT Manager and Office Administrator.
- The school web site complies with the school's guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, office@kaps.croydon.sch.uk. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

**Learning platform:**

- Uploading of information on the schools' Learning Platform / virtual learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the schools MLE will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved and closed systems, such as the Learning Platform;
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' Learning Platform for such communications.

**CCTV:**

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

**The use of Digital Images and Video**

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your child.

We follow the following rules for any external use of digital images:

**If the pupil is named, we avoid using their photograph.**

**If their photograph is used, we avoid naming the pupil.**

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staffs are not allowed to take photographs or videos on their personal equipment.

---

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity;
  e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / guardian.

- Your child's image being used for presentation purposes around the school;
  e.g. in class or wider school wall displays or PowerPoint© presentations.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;
  e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website.
  In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

**The use of Social Networking and On-line Media**

This school asks its whole community to promote the 3 commons approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

*How do we show common courtesy online?*

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

*How do we show common decency online?*

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

*How do we show common sense online?*

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.
*(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)*
In serious cases we will also consider legal options to deal with any such misuse.
The whole school community is reminded of the CEOP report abuse process:
https://www.thinkuknow.co.uk/parents/

**Resources for Parents**
http://www.saferinternet.org.uk/advice-and-resources/a-parents-guide
http://parents.vodafone.com/
Childnet Guide for Parents on Social Networking
How to set up Facebook Privacy Controls
Sample Family Online Safety Contract
A Parent's Guide to Facebook by Anne Collier and Larry Magid *February 2012*
A Guide to Facebook Security For Young Adults, Parents, and Educators
You Tube - safe search settings

**Appendix 3**

| | | |
|---|---|---|
| | **Kensington Avenue Primary School (KAPS)** | |
| | **AUP review Date** | **October 2017** |
| | **Date of next Review** | **October 2018** |
| | | |

**Acceptable Use Policy (AUP):**

**Key Stage 2 Children**

This document is to provide some guidelines to ensure that you stay safe and act responsibly when using ICT/Computing. When we talk about ICT/Computing, we are talking about computers, laptops, and everything else including cameras, USB microphones and other devices. By using the ICT/Computing in school, you have agreed to follow these rules. Your teacher will talk about these rules before you sign them. If you have any questions, please ask your teacher or Nadia.

- At all times, I will think before I click (especially when deleting or printing)
- When using the internet, I will think about the websites I am accessing
- If I find a website or image that is inappropriate, I will tell my teacher straight away
- When communicating online (e.g. in blogs) I will think about the words that I use and will not use words that may offend other people
- When communicating online, I will only use my first name and not share personal details such as my email address or phone number
- I understand that people online might not be who they say they are
- I will not look at other people's files or documents without their permission
- I will not logon using another person's account without their permission
- I know that the teachers can, and will, check the files and websites I have used
- I will take care when using the computers and transporting equipment around
- I will keep my usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents or teachers
- I will log off a computer when I am finished
- I will not install any software or hardware (including memory sticks) without permission from a teacher
- I understand that if I am acting inappropriately then my parents may be informed

Signature..... Date.....

Name..... Class.....

| | | |
|---|---|---|
| | **Kensington Avenue Primary School (KAPS)** | |
| | **AUP review Date** | **October 2017** |
| | **Date of next Review** | **October 2018** |
| | | |

**Acceptable Use Policy (AUP):**

**Key Stage 1 Children**

These rules have been written to make sure that you stay safe when using the computers. This includes cameras and microphones too. By using the ICT in school, you have agreed to follow these rules. Your teacher will talk about these rules before you sign them. If you have any questions, please ask your teacher or Nadia.

The Golden Rule: **Think before you click**

☺ I will be careful when going on the internet and will only use the internet when a teacher is with me.

☺ I will tell a teacher if I see something that upsets me.

☺ I know people online might not be who they say they are.

☺ I will be polite when talking to people or writing online.

☺ I will think before I print or delete.

☺ I will be careful when using or carrying equipment.

☺ I will keep my password secret, but I can tell my family.

☺ I will remember to log off properly when I am finished on a computer.

☹ I won't tell anyone any personal details like my phone number or last name.

☹ I won't logon using someone else's username.

☹ Never put water bottles on the table when using ICT.

Name..... Class.....

Signature..... Date.....

**Data Protection Act 1998**

**WHAT IS PERSONAL DATA?**

Personal data is any information that relates to a living individual.

**HOW DOES IT AFFECT SCHOOLS?**

Schools must register all personal data they hold and state the purposes for which it is required to be held. The fee for notification is now £35 and is renewable annually. Under the 1998 Act, as was the case with the 1984 Act, all processing undertaken by schools must be fair and lawful, accurate and up-to-date, and the data held must be adequate, relevant, not excessive and be held for no longer than is necessary. This means when personal data becomes out of date, or no longer relevant to the purpose for which it was originally collected, it must be destroyed. Holding on to the data may result in the school contravening the new Act.

**CONDITIONS FOR PROCESSING PERSONAL DATA**

Personal data should only be processed (that is, used) if one of several conditions apply including:
_ an individual has given their consent
_ the processing is part of a contract
_ there is a legal obligation to process the data or
_ the processing is necessary to protect the individual

If none of the conditions apply there are no legitimate grounds to process the data. Anyone found to be processing data in these circumstances would be contravening the Act. Contravening the Act is a criminal offence, which is punishable by a maximum fine of £5,000 in the Magistrates court and an unlimited fine in the Crown court.

**NEW CATEGORY OF SENSITIVE DATA**

The new Act also defines "sensitive personal data" for the first time including racial, ethnic origin, political affiliations, religious or other beliefs. This type of data demands greater protection and one of the following must be true before the data can be processed:
_ an individual has given their explicit consent
_ you have a legal requirement to process the data
_ it is necessary to protect the vital interests of the individual
Explicit consent means fully informing the individual of the relevant facts in relation to the proposed processing and getting their written consent.

**WHAT ABOUT PROTECTING PERSONAL DATA?**

The new Act also makes it mandatory to ensure that appropriate technical and organisational measures are taken to prevent unauthorised access to or disclosure of data. This includes accidental loss or destruction of, or damage to, personal data. This means for example that sensitive data must be protected from unauthorized access by using password-based access control.
If a request for information under the Act is refused or ignored, the matter can be referred to the Data Protection Commissioner or an application for disclosure can be made to a court.

**PRINCIPLES OF THE NEW ACT**

There are eight over-arching principles of the 1998 Act:

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Personal data shall be accurate and, where necessary, kept up to date
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
6. Personal data shall be processed in accordance with the rights of data subjects under the Act
7. 7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

**WHAT HAPPENS IF THE ACT IS CONTRAVENED?**

If anyone knowingly or recklessly contravenes the new Act, any individual suffering damage or distress as a result is entitled to claim compensation through the courts.
The courts may also prosecute the person responsible for committing the offence under the Act. Furthermore, if a Court rules that data relating to an individual is inaccurate, then the school can be required to delete or amend the data.

**WHO IS RESPONSIBLE FOR DATA PROTECTION?**

Everyone who handles personal data as part of their job needs to be aware of his or her responsibilities under the Data Protection Act, 1998. As was the case with the 1984 Act, individual employees are personally liable (a fine and a criminal record) for breaches of the Act if they disregard instructions given on the proper handling of personal data.

**STAFF TRAINING – REQUIREMENTS OF THE ACT**

All staff dealing with personal data should be aware of the requirements of the Act and be familiar with how to conform to these in their daily work. You may find it helpful for example to use this leaflet as a briefing note for new members of staff and as a ‘refresher’ document for existing staff.

**PUBLICATION OF WEB PAGES**

- Only access the Internet via a PC which has been expressly set up within the school for that purpose.
- Publication of personal information or images of individuals on any Web Site schools develop should only be done if the written consent of the individuals concerned has been given.

**USE OF ELECTRONIC MAIL AND THE INTERNET - DATA PROTECTION REQUIREMENTS**

The use of electronic mail and the Internet by schools also raises certain Data Protection issues. As an absolute minimum please bear the following points in mind:

- Do not include personal or confidential information in the text of emails (or as an email attachment) to be sent outside the school unless appropriate encryption is applied to protect it.
- Email should never be treated as a secure method of communication when dealing with personal data as defined by the Data Protection Act.

**NEW CCTV CODE OF PRACTICE**

CCTV cameras are increasingly being used by organisations for a variety of monitoring and surveillance purposes. In recognition of this the Data Protection Commissioner has issued a CCTV Code of Practice to comply with the provisions of the 1998 Data Protection Act. The code offers practical advice in helping schools to meet their legal obligations.

What does the Code of Practice cover?
The Code sets out the legal standards and provides guidance on good practice in addition to advice on practical matters such as suitable sighting of CCTV cameras, procedures for informing people what is happening, guidance on what can happen to the images and how long you should retain them.

What is required to ensure schools' use of CCTV complies with the Act and the Code of Practice?
CCTV systems used on school premises must be operated in accordance with the provisions of the Data Protection Act, 1998. Responsibility for adhering to the relevant requirements here rests with the individual school concerned.
Schools have a legal duty to notify the Data Protection Commissioner of the purposes for which the CCTV equipment is used. Appropriately worded signs must also be on display on the school site pointing out that such equipment is in use and the purpose for it being in operation.
The recommended wording for a notice is 'CCTV surveillance equipment is in operation in this area. Images are being recorded for the purposes of crime prevention, for ensuring the safety of school employees and visitors, and for protecting School premises and property.
The notice should also include both details of the organisation responsible for the scheme e.g. the name of the school and the specific contact point for further information (usually the head teacher).

**ACCESS TO PERSONAL DATA – PUPIL RIGHTS**

The Data Protection Act gives all school students, regardless of age, the right of access to their school pupil records. Requests to see or receive copies of records should be made in writing to the head teacher. In addition to the right to be given a copy of the educational record, students are entitled to be given a description of the personal data which makes up the record, together with details of the purposes for which the data are processed, the sources of the data (if known) and the individuals or organizations to which the data may have been disclosed.
A period of up to 15 school days is allowed in which to respond to a subject access request. (The equivalent period for other types of record is up to 40 days.) If asked to provide a hard copy of the record, a fee may be charged according to the number of pages. Students may be asked for information to verify their identity if necessary, for instance in the case of former pupils who may not be currently known to the school. They may also be asked for information necessary to locate the data held about them. For instance a student may be asked to supply the dates between which he or she attended the school.

While in principle students have a right of access to the whole of their educational records, in exceptional cases some information may be withheld. The main exemptions are for information which might cause harm to the physical or mental health of the student or a third party, information which may identify third parties (for example other pupils, although not teachers), and information which forms part of some court reports. Information may also be withheld if in that particular case it would hinder the prevention and detection of crime or the prosecution or apprehension of offenders to provide it. If students are incapable of understanding or exercising their own rights under the Data Protection Act, (for instance because they are too young), parents can, of course, make subject access requests on their behalf.

**ACCESS TO PERSONAL DATA – PARENTAL RIGHTS**

In addition to the subject access right which can be exercised by pupils or by parents acting on behalf of pupils, parents have their own independent right of access to the official educational records of their children. In essence the information to which parents are entitled and the exemptions are the same as for pupils, although there is no parental right of access to information which does not form part of the official record. Requests to see or receive copies of the educational records of their children should be made in writing.

**WHAT ABOUT MANUAL FILING SYSTEMS DATA?**

A major change under the new Act is that it now makes certain data held in manual or paper form subject to the data protection rules. For the first time individuals whose personal information is recorded manually will, in some cases, have a right to see that information and make corrections if necessary.

**WHAT IS A STRUCTURED MANUAL FILING SYSTEM?**

This means any set of information relating to an individual that is readily accessible either by reference to the individual or criteria relating to the individual.
The Data Protection Act, 1998 came into force on 1st March, 2000. This leaflet provides a summary of its key points and operating principles. Please use it as a guide to ensure that your school adheres to legal requirements in this important area. The new Act carries forward elements from the previous Data Protection Act, introduced in 1984, and imposes stringent conditions on the way 'data controllers' such as schools hold or process personal data.

**Liz Johnston belb October 2004**
**Board of Governors Awareness Sessions.**