KESTON SCHOOL	Name of School	Keston Primary School
	Policy review Date	Autumn 2015
	Date of next Review	Autumn 2016
	Who reviewed this policy?	Computing leader – Rebecca East Senior Leadership Team Governors

Policy: The Acceptable Use of the Internet and related Technologies

Our e-Safety Policy has been written by the school, building on the London Grid for Learning (LGfL) exemplar policy and Becta guidance. It has been agreed by the senior management and approved by Governors. It will be reviewed annually.

Context:

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005

The staff and governors of Keston primary School recognise they have a duty to ensure that all students are able to make a valuable contribution to society and this is impossible to achieve if we do not ensure that students develop and apply their Computing capability effectively in their everyday lives.

The school is aware of its responsibilities in ensuring that ICT usage by all network users is responsible, safe and secure. There are relevant and comprehensive policies in place which are understood and adhered to by many network users.

The Green Paper *Every Child Matters*[i] and the provisions of the *Children Act 2004*[ii], *Working Together to Safeguard Children*[iii] sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

1. The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites
- Video broadcasting sites
- Chat Rooms
- Gaming Sites
- Music download sites
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are ‘Internet ready’.
- Smart phones with e-mail, web functionality and cut down ‘Office’ applications.

2. Whole school approach to the safe use of ICT

Creating a safe Computing learning environment includes three main elements at this school:

- An effective range of technological tools;

- Policies and procedures, with clear roles and responsibilities;

- A comprehensive e-safety education programme for pupils, staff and parents.

3. Roles and Responsibilities

E-safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The head teacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-safety has been designated to a member of the senior management team.

E-safety is overseen by Claire Murphy (Head teacher) and co-ordinated by Rebecca East (Computing subject leader).

Our e-safety Coordinator ensures she keeps up to date with e-safety issues and guidance through liaison with the Local Authority e-safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP)[iv]. The schools’ e-safety coordinator ensures that senior management and Governors are updated as necessary.

Governors need to have an understanding of e-safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on e-safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil information/photographs and use of website;
- e-Bullying / Cyberbullying procedures;
- their role in providing e-Safety education for pupils;

Staff are reminded / updated about e-safety matters at least once a year. E-safety is also delivered in a whole school assembly. All staff agree to the Acceptable Use Policy a copy of which is held by the staff member and the school. *(Appendix I)*

He school includes e-safety in the curriculum and ensures that every pupil has been educated about safe and responsible use. Pupils need to know how to control and minimise online risks and how to report a problem.

4. Communications

How will the policy be introduced to pupils?

Discussion: Many pupils are very familiar with the culture of new technologies, they can be involved them in designing the School e-safety Policy, possibly through a student council. Pupils' perceptions of the risks may not be mature; the e-safety rules may need to be explained or discussed.

Consideration must be given as to the curriculum place for teaching e-safety.

- E-safety training will be incorporated into the school INSET to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede Internet access.
- An e-safety lesson will be taught each term to cover the use of the internet at home and at school.

How will the policy be discussed with staff?

Discussion: It is important that all staff feel confident to use new technologies in teaching. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies

Staff must understand that the rules for information systems misuse. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with the Computing subject leader to avoid any possible misunderstanding.

ICT use is widespread and all staff including administration, caretaker, governors and helpers should be included in appropriate awareness raising and training. Induction of new staff should include a discussion of the school's e-safety Policy.

- Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

How will parents' support be enlisted?

Discussion: Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school may be able to help parents plan appropriate supervised use of the Internet at home.

- Internet issues will be handled sensitively, and parents will be advised accordingly.

5. How will complaints regarding e-safety be handled?

The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview with e-safety Coordinator / Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system];
- referral to LA / Police.

Our e-safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Section 2 - Managing the Internet Safely

Why is Internet access important?

The Internet is an essential element in 21st century life for education, business and social interaction. Computing skills and knowledge are vital to access life-long learning and employment; indeed Computing is now seen as a functional, essential life-skill along with English and mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All pupils should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet provides many benefits to pupils and the professional work of staff through, for example:

- access to world-wide educational resources, including museums and art galleries;
- access to experts in many fields for pupils and staff;
- educational and cultural exchanges between pupils world-wide;
- collaboration between pupils, professionals and across sectors;
- access to learning wherever and whenever convenient.

The Internet enhances the school's management information and business administration systems through, for example:

- communication systems;
- improved access to technical support, including remote management of networks and automatic system updates;
- online and real-time ‘remote’ training support;
- secure data exchange between local and government bodies.

The risks

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be considered inappropriate and restricted elsewhere.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk. This must be within a ‘No Blame’, supportive culture if pupils are to report abuse.

Technical and Infrastructure:

This school:

- Maintains the filtered broadband connectivity through the LGfL and so connects to the ‘private’ National Education Network;

- Works in partnership with the LA to ensure any concerns about the system are communicated to LGfL so that systems remain robust and protect students;
- Ensures their network is ‘healthy’ by having health checks annually on the network;
- Utilises caching as part of the network set-up;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies;
- Ensures the Systems Administrator / network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Never allows pupils access to Internet logs;
- Never sends personal data over the Internet unless it is encrypted or otherwise secured;
- Never allows personal level data off-site unless it is on an encrypted device;
- Uses ‘safer’ search engines with pupils where appropriate

Policy and Procedures:

This school:

- Supervises pupils’ use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access;
- We use the pan-London LGfL / Synetrix filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- We have additional user-level filtering, so adapt filtering to the age of the pupils;
- Staff preview all sites before use [where not previously viewed and cached] or only use sites accessed from managed ‘safe’ environments such as the Learning Platform;
- Plans the curriculum context for Internet use to match pupils’ ability, using child-friendly search engines where more open Internet searching is required;
- Is vigilant when conducting ‘raw’ image search with pupils e.g. Google image search;
- Informs users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the Computing leader. Our systems administrators report to LA / LGfL where necessary;
- Only uses approved or checked webcam sites;
- Requires pupils from Key Stage 1 and 2, to sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme; (*Appendix II and Appendix III)*
- Uses closed / simulated environments for e-mail with Key Stage 1 pupils;
- Requires all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file;
- Makes clear all users know and understand what the ‘rules of appropriate use’ are and what sanctions result from misuse – through staff meetings and teaching programme;
- Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;

- Ensures the named child protection officer has appropriate training;
- Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their daughter's / son's entry to the school;
- Makes information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Education and training:

This school:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report abuse;
- Has a clear, progressive e-safety education programme throughout all Key Stages, built on LA / London / national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

    - to STOP and THINK before they CLICK *(See Appendix IV)*
    - to discriminate between fact, fiction and opinion;
    - to develop a range of strategies to validate and verify information before accepting its accuracy;
    - to skim and scan information;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know some search engines / web sites that are more likely to bring effective results;
    - to know how to narrow down or refine a search;
    - to understand how search engines work;
    - to understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to know not to download any files – such as music files - without permission;

    - to have strategies for dealing with receipt of inappropriate materials;

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;
- Ensures staff know how to encrypt data where the sensitivity requires and that they understand data protection and general ICT security issues linked to their role and responsibilities;
- Makes training available annually to staff on the e-safety education program;
- Runs a rolling programme of advice, guidance and training for parents, including:
    - Information leaflets; in school newsletters; on the school web site;
    - demonstrations, practical sessions held at school;
    - distribution of ‘think u know’ for parents materials
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents.

Section 3 - Managing e-mail

E-mail is now an essential means of communication for staff in our schools and increasingly for pupils and homes. Directed e-mail use in schools can bring significant educational benefits through increased ease of communication between staff and between pupils.
However, un-regulated e-mail can provide a means of access to a pupil that bypasses the traditional school physical boundaries.

This school:

- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for any communication with the wider public.
- If one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law we will contact the police.
- Accounts are managed effectively, with up to date account details of users
- Messages relating to or in support of illegal activities may be reported to the authorities.

Pupils:

- We only use LGfL 'safemail' with pupils.
- Pupils can only use the LGfL / school domain e-mail accounts on the school system.
- Pupils are introduced to, and use e-mail as part of the ICT scheme of work.
- Pupils are taught about the safety and 'netiquette' of using e-mail i.e.
    - not to give out their e-mail address unless it is part of a school managed project or someone they know and trust and is approved by their teacher or parent/carer;
    - that an e-mail is a form of publishing where the message should be clear, short and concise;
    - that any 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;
    - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
    - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    - the sending of attachments should be limited;
    - embedding adverts is not allowed;
    - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
    - not to respond to malicious or threatening messages,
    - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
    - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
    - that forwarding 'chain' e-mail letters is not permitted;

- Pupils sign the school Agreement Form to say they have read and understood the e-safety rules (appendix II/III), including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff use LA or LGfL e-mail systems for professional purposes;
- Access in school to external personal e-mail accounts may be blocked;
- Staff sign the appropriate LA / school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with. *(Appendix I)*

Section 4 – Use of Digital and Video Images

In this school:

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- Uploading of information is restricted to the website team.
- The school web site complies with the school's guidelines for publications;
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- 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 school; *(see Appendix 5)*
- Digital images /video of pupils are stored in the 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 use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
- We do not 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;
- Pupils are only able to publish to their own 'safe' web-portal on the LGfL in school;
- Pupils are taught about how images can be abused in their e-safety education programme;
- Pupils are taught to be very careful about placing any personal photos on any 'social' online space and that they should not post images or videos of others without permission.

Section 5 – Managing equipment

The computer system / network is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

To ensure the network is used safely this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet and email access and can be given an individual network log-in username and password;
- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find;
- Makes clear that pupils should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;
- Makes clear that no one should log on as another user – if two people log on at the same time this may corrupt personal files and profiles;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We automatically remotely switch off all computers at the end of the day;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;
- Maintains equipment to ensure Health and Safety is followed;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their Shibboleth compliant username and password.
- Uses the DfES secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA;

- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the school ICT systems regularly with regard to security.

Section 6 – Handling of Infringements

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

Students

Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Use of unauthorised instant messaging / social networking sites

Category A sanctions

- Referral to phase leader or member of the leadership team.

Category B infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued use of unauthorised instant messaging / chat rooms, social networking sites, Newsgroups
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

Category B sanctions

- Referral to head teacher or deputy head teacher
- Removal of Internet access rights for a period
- Contact with parent

Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

Category C sanctions

- Referral to head teacher or deputy head teacher
- Referral to e-safety coordinator

- Removal of internet rights for a more extended period
- Contact with parents

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform the Local Authority / Synetrix as appropriate

Category D infringements

- Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

Category D sanctions

- Referred to Head Teacher
- Contact with parents
- Possible exclusion
- Refer to Community Police Officer
- LA e-safety officer

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider

Staff

Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.
- Not implementing appropriate safeguarding procedures.
- Any behaviour on the world wide web that compromises the staff members professional standing in the school and community.
- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software on network.

*[Sanction - **referred to line manager / Headteacher**. Warning given.]*

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

*[Sanction – **Referred to Headteacher / Governors and follow school disciplinary procedures;** report to LA Personnel/ Human resources, report to Police]*

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Child Pornography

In the case of Child Pornography being found, the member of staff should be **immediately suspended** and the Police should be called:

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

How will staff and students be informed of these procedures?

- They will be fully explained and included within the school's e-safety / Acceptable Use Policy. All staff will be required to sign the school's e-safety Policy acceptance form;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate e-safety / acceptable use form;
- The school's e-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.
- Staff are issued with the 'What to do if?' guide on e-safety issues,

Appendix I

	Name of organisation	**Keston Primary School**
	AUP review Date	**Autumn 2015**
	Date of next Review	**Autumn 2016**
	Who reviewed this AUP?	**Rebecca East – Computing co-ordinator**

Acceptable Use Policy (AUP):

Adults working with children agreement form

This covers use of digital technologies in Keston Primary School: including email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- 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 allow unauthorised individuals to access any of school/ LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities – there should be absolutely no private online contact between professionals and any young person with whom they have a work-related relationship.
- I understand that any / my personal online communication tools must not be used with service users and will not communicate or 'befriend' any service user using such methods – friend requests from children and young people, or their families, should be declined by explaining it is against the organisations policy to do so.
- I will only use the approved email system for any email communication related to work at school. This is currently: LGfL Staffmail.
- I will only use other school approved communication systems for any communication with young people or parents/carers.
- I will not browse, download or send material that could be considered offensive to colleagues I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.

- 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 school’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 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. Staff and volunteers must have the appropriate security on their profiles to stop anyone viewing them that they are not friends with.
- I will not create web pages, groups or contact lists concerning professional activities carried out on behalf of the organisation without the expressed permission. Work related accounts may be used with management approval. Such sites should be able to be checked and audited by managers.
- I agree and accept that any computer or laptop loaned to me by school, 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 school 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 schools 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 school/ 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 understand that it is my duty to support a whole organisation safeguarding approach and I will alert the school’s 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.

Acceptable Use Policy (AUP): ‘Staff’ agreement form

User Signature

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 school’s most recent e-safety policies.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school’s ICT resources and systems.

Signature .... Date ....

Full Name .... (printed)

Job title ....

Keston Primary School ....

Authorised Signature

I approve this user to be set-up.

Signature .... Date ....

Full Name .... (printed)

Appendix II

Infants Acceptable Use Agreement

S

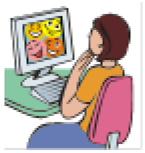
I will only use the Internet with an adult.

A

I will only click on programme icons that are on the desktop.

F

I will only send friendly and polite messages.

E 

If I see something I don't like on a screen, I will always tell an adult.

Appendix III

KS2 Acceptable Use Agreement

These rules will keep us safe and help us to be fair to others.

- We will only use the school's computers for schoolwork and homework.
- We will only edit or delete our own files and not look at, or change, other people's files without their permission.
- We will keep our logins and passwords secret.
- We will not bring files into school without permission or upload inappropriate material to our workspace.
- We are aware that some websites and social networks have age restrictions and we should respect this.
- We will not attempt to visit Internet sites that we know to be banned by the school.
- We will only e-mail people we know, or a responsible adult has approved.
- The messages we send, or information we upload, will always be polite and sensible.
- We will not open an attachment, or download a file, unless we know and trust the person who has sent it.
- We will not give our home address, phone number, send a photograph or video, or give any other personal information that could be used to identify us, our family or friends, unless a trusted adult has given permission. We will never arrange to meet someone we have only ever previously met on the Internet, unless our parent/carer has given us permission and we take a responsible adult with us.
- If we see anything we are unhappy with or receive a message we do not like, we will not respond to it but will show a teacher / responsible adult.

We have read and understand these rules and agree to them.

Appendix IV

12 rules for responsible ICT use at Keston Primary

Keeping safe: stop, think, before you click!

These rules will keep everyone safe and help us to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only delete my own files.
- I will not look at other people's files without their permission.
- I will not tell anyone outside of the school my login and password.
- I will not bring files into school without permission.
- I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school.
- I will only e-mail people my teacher has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I have permission.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet or by email, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.

Appendix V

E-safety agreement form: parents

Parent / guardian name: ________________________________

Pupil name(s): ____

As the parent or legal guardian of the above pupil(s), I grant permission for my daughter or son to have access to use the Internet, LGfL e-mail* and other ICT facilities at school.

I know that my daughter or son has signed an e-safety agreement form and that they have a copy of the 12 ‘rules for responsible ICT use’.

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 will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email*, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child’s computer files, and the Internet sites they visit, and that if they have concerns about their e-safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child’s e-safety.

Parent / guardian signature: _____________________________

Date: ___/___/___

Use of digital images - photography and video: I also agree to the school using photographs of my child or including them in video material, as described in the document ‘Use of digital and video images’. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Parent / guardian signature: _______________________ Date: ___/___/___

Use of digital images - photography and video

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

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 include:

- Your child being photographed (by the classroom teacher, teaching assistant or another child) as part of a learning activity;
  e.g. photographing children at work and then sharing the pictures on the Interactive whiteboard in the classroom allowing the children to see their work and make improvements.

- Your child's image for presentation purposes around the school;
  e.g. in school wall displays and PowerPoint© presentations to capture images around the school or in the local area as part of a project or lesson.

- 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 image could appear in the media if a newspaper photographer or television film crew attend 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.

Further information for parents on e-Safety can be found at:
http://www.parentscentre.gov.uk/usingcomputersandtheinternet/linksbytopic/