KITWELL PRIMARY SCHOOL AND NURSERY CLASS

Online Safety Policy

Ratified by the Governing Body
To be reviewed

Our Vision

Kitwell Primary School and Nursery Class embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, Kitwell aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

Aims

This policy document sets out the school's aims, principles and strategies for using the Internet and protecting pupils.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information, and communications with wider communities and business administration systems.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

Staff and pupils have access to web sites worldwide offering educational resources, news and current events. There will be opportunities for discussion and exchange of information within the school community and others worldwide. Staff have the opportunity to access educational materials and good curriculum practice, to communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the Local Authority and Department for Education (DfE); receive up to data information and participate in government initiatives such as National Education Network (http://www.nen.gov.uk/). The Internet is also used to enhance the school's management information and business administration systems.

Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the school and to personal devices owned by adults and young people while on the school premises.

Related Documents:

Acceptable Use Policy for Adults
Acceptable Use Policy for Young People
Data Protection Policy
Behaviour Policy
Anti-bullying Policy
Birmingham City Council Internet Use Policy, Internet Use Code of Practice and Email Use Policy (linked from www.bgfl.org/esafety)
AUPs in context: Establishing safe and responsible behaviours
Policy Owner (DSL and Online Co-ordinator): P. D. Kendrick
Implementation Date: Autumn 2016
Review Date: Autumn 2017

Publicising online safety

Effective communication across the school community is key to achieving the school vision for safe and responsible citizens. To achieve this we will:

- Make this policy, and related documents, available on the school website at: http://www.kitwellschool.com/
- Introduce this policy, and related documents, to all stakeholders at appropriate times. This will be at least once a year or whenever it is updated
- Post relevant online safety information in all areas where computers are used
- Provide online safety information at parents' evenings, through the school newsletter, through the school website and blogs and through the 'Kitwell Chronicle'.

Roles and Responsibilities

The Head and Governors have ultimate responsibility for establishing safe practice and managing online safety issues at our school. The role of online safety co-ordinator has been allocated to P. D. Kendrick, our Designated Senior Leader for child protection and a member of the senior management team. They are the central point of contact for all online safety issues and will be responsible for day to day management. However, all members of the school community have certain core responsibilities within and outside the school environment. They should:

- Use technology responsibly
- Accept responsibility for their use of technology
- Model best practice when using technology
- Report any incidents to the online safety coordinator using the school procedures
- Understand that network activity and online communications are monitored, including any personal and private communications made via the school network.
- Be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action

Additional roles and responsibilities are discussed in the NAACE document - AUPs in context: Establishing safe and responsible behaviours and also available at http://www.bgfl.org/esafety. These will be communicated to the relevant groups at appropriate times.

Physical Environment / Security

The school endeavours to provide a safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system consulting with the LA where appropriate.

- Anti-virus software is installed on all computers and updated regularly;

- Central filtering is provided and managed by Link2ICT. All staff and students understand that if an inappropriate site is discovered it must be reported to the online safety co-ordinator who will (if deemed necessary) report it to the Link2ICT Service Desk to be blocked. All incidents will be recorded in the online safety log for audit purposes;
- Requests for changes to the filtering will be directed to the online safety co-ordinator in the first instance who will forward these on to Link2ICT or liaise with the Head as appropriate. Change requests will be recorded in the online safety log for audit purposes;
- The school uses Policy Central Enterprise Version 6 on all school owned equipment to ensure compliance with the Acceptable Use Policies;
    - Pupils' use is monitored by P. Kendrick
    - Staff use is monitored by the Head and P. Kendrick
- All staff are issued with their own username and password for network access. Visitors / supply staff are issued with temporary IDs and the details recorded in the school office;
- All pupils use year group logon IDs for their network access;
- For email use (when required) all pupils are issued with their own username and password and understand that this must not be shared. This will take place once the relevant parents and carers are informed.

Mobile / emerging technologies

- Teaching staff at the school are provided with a laptop for educational use and their own professional development. All members of staff understand that the Acceptable Use Policies apply to this equipment at all times;
- To ensure the security of the school systems, personal equipment is generally not permitted to be connected to the school network unless formal approval has been sought from the Head Teacher and the ICT Manager;
- Staff understand that they should use their own mobile phones sensibly and in line with school policy;
- Pupils are not allowed to bring their own mobile phones/devices into school;
- The Educations and Inspections Act 2006 grants the Head the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Head will exercise this right at their discretion
- Where photos/videos of children/staff are taken on personal devices, it is strongly recommended that the photos/videos are removed before the end of the day and stored on the school network;
- Visiting teachers/visiting adults/students are not allowed to take pictures / videos on personal devices unless permission has been sought from the relevant shareholders;
- New technologies are constantly being re-evaluated and risk assessed for their educational benefits before they are introduced to the school community.

E-mail

The school e-mail system is provided, filtered and monitored by Google Apps for Education education and is governed by Google Apps Education Email Use Policy at http://www.google.com/apps/intl/en/terms/use_policy.html

- All staff are given a school e-mail address and understand that this must be used for all professional communication;
- Key stage 1 pupils may be given access to class based e-mail accounts that are monitored by the class teacher;
- Keys stage 2 pupils are given (where necessary, and required by the school ICT curriculum) a school e-mail address that can be used for class based activities. Parents and carers will be informed if this is going to take place;
- Where appropriate, all pupils can be given a school e-mail address that can be used for educational purposes. Parents and carers will be informed if this is going to take place;
- Everyone in the school community understands that the e-mail system is monitored and should not be considered private communication;
- Guidance is given to the school community around how e-mail should be structured when using school e-mail addresses;
- Staffs are allowed to access personal e-mail accounts on the school system outside directed time and understand that any messages sent using the school equipment should be in line with the e-mail policy. In addition, they also understand that these messages will be scanned by the monitoring software;
- Pupils may be given the opportunity to check their own e-mail outside directed time and understand that any messages sent using the school equipment should be in line with the e-mail policy. In addition, they also understand that these messages will be scanned by the monitoring software and also the school network administrator;
- Everyone in the school community understands that any inappropriate e-mails must be reported to the class teacher / online safety co-ordinator as soon as possible.

Published content

The Head takes responsibility for content published to the school web site but delegate's general editorial responsibility to *P. Kendrick*. Class teachers are responsible for the editorial control of work published on the school Blogs.

- The school will hold the copyright for any material published on the school web site or will obtain permission from the copyright holder prior to publishing with appropriate attribution;
- The school encourages the use of e-mail to contact the school via the school office / generic e-mail addresses / staff e-mail addresses;
- The school does not publish any contact details for the pupils;
- The school encourages appropriate, educational use of other Web 2.0 technologies and where possible embeds these in the school web site or creates a school account on the site (e.g. Blogs, Wordpress).

Digital Media

We respect the privacy of the school community and will obtain written permission from staff, parents, carers or pupils before any images or video are published or distributed outside the school.

- Photographs will be published in line with NAACE guidance and not identify any individual pupil (http://cnp.naace.co.uk/system/files/data_protection_in_schools.pdf);
- Students' full names will not be published outside the school environment;
- Written permission will be obtained from parents or carers prior to pupils taking part in external video conferencing;
- Students understand that they must have their teachers permission to make or answer a video conference call;
- Supervision of video conferencing will be appropriate to the age of the pupils.

Social Networking and online communication

The school is constantly reviewing the use of social networking sites and online communication and currently does not allow access to Social Networking Sites. Most popular sites are currently blocked through the BGFL filtering system.

Kitwell will provide guidance to the school community on how to use these sites safely and appropriately in the home environment. This includes:-

- not publishing personal information;
- not publishing information relating to the school community;
- how to set appropriate privacy settings;
- how to report issues or inappropriate content.

Un-moderated chat sites present an unacceptable level of risk and are blocked in school. Pupils are given age appropriate advice and guidance around the use of such sites.

Information pertaining to the above is provided to relevant shareholders at relevant times in a child's school career.

Staff are advised of the risks of putting private information into a public domain and also 'bringing school into disrepute' through the private use of social networking sites.

For the safety and the protection of all relevant parties: staff should NOT add/accept school pupils as friends on social networking sites.

The school currently has a Twitter account which can be accessed by parents directly through the school website. Parents are encouraged to become 'followers' of the Kitwell account. 'Followers' of the Kitwell account can be accessed directly though the Twitter home page. For this reason, parents are advised that they should only follow the Kitwell account should their own account contain no 'tweets' which contain material or language not appropriate for children of primary school age. Any 'follower' accounts containing inappropriate material or language will be blocked from accessing the school Twitter account and further action may be taken.

Educational Use

- School staff model appropriate use of school resources including the Internet.
- All activities using the Internet, including homework and independent research topics, will be tested first to minimise the risk of exposure to inappropriate material;
- Where appropriate, links to specific web sites will be provided instead of open searching for information. Pupils will be taught how to conduct safe searches of the Internet as part of Computing lessons;
- Where pupils are allowed to freely search the Internet e.g. using search engines, staff should be vigilant in monitoring the content of the websites the children visit;
- Teachers will be responsible for their own classroom management when using ICT equipment and will remind pupils of the Acceptable Use Policies before any activity;
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of the information.

The Use of the Internet to Enhance Learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Access to social media and social networking sites is controlled by BCC.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor BCC can accept liability for the material accessed, or any consequences of Internet access.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Head teacher and Governors will ensure that the Internet policy is implemented and compliance with the policy monitored.

Pupil Responsibilities

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

- A planned online safety programme should be provided as part of Computing / PHSE / other lessons and should be regularly revisited - this will cover both the use of ICT and new technologies in school and outside school
- Key online safety messages should be reinforced as part of a planned programme of assemblies or lessons
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils and parents will sign the Internet/acceptable use policy (see appendix)
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils understand and follow the school Online safety and Acceptable Use Policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- The pupil acceptable usage agreement will be displayed in the computer suite.
- Pupils will be informed that Internet use will be monitored (Policy Central Enterprises Version 6).
- Instruction in responsible and safe use should precede Internet access.

Staff Responsibilities

- All staff must accept the terms of the 'Birmingham Education Service Policy for Acceptable use of the internet'
- Staff will ensure they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP). (See appendix)
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by the Senior leadership team.
- All staff need have an up to date awareness of online safety matters and of the current school online safety policy and practices
- Staff must report any suspected misuse or problem to the ICT Co-ordinator/ DSL/ Online safety coordinator or Head teacher for investigation / action / sanction
- Digital communications with pupils (Virtual Learning Environment - VLE) should be on a professional level and only carried out using official school systems
- Staff are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined as part of induction procedures.

Online safety training

The ICT Manager and Online safety Co-odinator will work together to carry out the implementation of the following processes:-

- There is an induction process and mentor scheme available for new members of staff;
- Educational resources are reviewed by subject managers and disseminated through curriculum meetings / staff meetings / training sessions;
- Online safety is embedded throughout the school curriculum and visited by each year group;
- Pupils are taught how to validate the accuracy of information found on the Internet;
- Parents sessions will be run in conjunction with other school activities (e.g. INSPIRE workshops) and will provide appropriate advice and guidance.

Data Security / Data Protection

Personal data will be recorded, processed, transferred and made available in line with the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Process for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Data is stored on the school systems and transferred in accordance with the NAACE Data Security Guidelines

Staff must ensure that they:

- At all times, take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged off' at the end of any session in which they are using personal data.

Sensitive personal pupil/staff data should never be taken off site without permission. In instances where permission is given, the personal data that is stored on personal computer systems, USB sticks or other removable media should adhere to the following:

- The data must be encrypted and password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device once it has been transferred or its use is complete.

Wider Community

Third party users of school equipment will be advised of the policies, filtering and monitoring that is in place. They will be issued with appropriate usernames and password that will be recorded in the school office.

Equal Opportunities

This online safety policy works in conjunction with the school Equal Opportunities policy.

Responding to incidents

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity, i.e.

- **Child sexual abuse images**
- **Adult material which potentially breaches the Obscene Publications Act**
- **Criminally discriminatory or prejudicial material**
- **Other criminal conduct, activity or materials**
- **Use of online materials to share or encourage radical or extreme points of view**

- Inappropriate use of the school resources will be dealt with in line with other school policies e.g. Behaviour, Anti-Bullying and Child Protection Policy.
- Any suspected illegal activity will be reported directly to the police. The Link2ICT Service Desk will also be informed to ensure that the Local Authority can provide appropriate support for the school;
- Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be referred directly to the Head;
- Breaches of this policy by staff will be investigated by the Head Teacher. Action will be taken under Birmingham City Council's Disciplinary Policy where a breach of professional conduct is identified. Incidents will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct. All monitoring of staff use will be carried out by at least 2 senior members of staff;
- Student policy breaches relating to bullying, drugs misuse, abuse and suicide must be reported to the nominated child protection representative and action taken in line with school anti-bullying and child protection policies. There may be occasions when the police must be involved;
- Serious breaches of this policy by students will be treated as any other serious breach of conduct in line with school Behaviour Policy. The Head Teacher will be made aware of – and may be asked to deal with - email alerts generated by PCE for students. For all serious breaches, the incident will be fully investigated, and appropriate records made on personal files with the ultimate sanction of exclusion reserved for the most serious of cases;
- Minor student offenses, such as being off-task visiting games or email websites will be handled by the teacher in situ by invoking the school behaviour policy;
- The Educations and Inspections Act 2006 grants the Head the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate.

Policy adapted from the Birmingham Model Policy by P. Kendrick – November 2015

Kitwell Primary School & Nursery Class

Wychbury Road, Bartley Green, Birmingham B32 4DL

Telephone: 0121 476 0694
Fax: 0121 476 1700
Email: enquiry@kitwell.bham.sch.uk
Web: www.kitwellschool.com

Headteacher: Mrs M Shevels

ICT Acceptable Use Policy/Online safety Rules

Dear Parents/Carers,

All pupils use computer facilities including internet access as an essential part of learning, as required by the National Curriculum (Computing). In order to ensure the safety of all pupils and staff, Kitwell Primary School has an 'Acceptable Use Policy' for Information and Communication Technology (ICT) equipment in school.

This Acceptable Use Policy (AUP) reflects the changing nature of ICT and the Computing curriculum. Please read the attached agreement form and 'E- Safety Rules' with your child and then sign the agreement form and return it to school.

We have included a copy of the 'Online safety Rules', which you may wish to display next to your home computer.

These Online safety rules stand until such a time as the demands of technology and the Computing curriculum require it to be adapted.

The full version of our Online safety policy is available to view on the school website. Our school website also has a page which gives up to date guidance for parents and children when using the Internet. Please visit our website at www.kitwellschool.com for further information. If you any questions about this, please don't hesitate to contact me at school.

Yours sincerely,

P. D. Kendrick

Mr. P Kendrick
Deputy Head Teacher
ICT Co-ordinator

Online safety Rules

These online safety Rules help to protect pupils and the school by describing acceptable computer use.

- We ask permission before using the internet.
- We tell an adult immediately if we see anything we are uncomfortable with.
- We immediately close any webpage we are not sure about.
- We keep our personal information and passwords private.
- We do not copy other people's work (text, music, images) without permission.
- We only email people an adult has approved.
- We only open emails sent by people we know.
- We send emails that are polite and friendly.
- We never arrange to meet anyone we don't know.
- We do not use instant messaging or chat rooms at school.
- We understand that we will only be allowed to use the internet if we are sensible and careful.
- We understand that our school can see everything that we do on a school computer.

Kitwell Primary School and Nursery Class

Online safety Pupil/Parent Agreement

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the online safety Rules have been understood.

Pupil's name:
Pupil's Agreement • I have read and I understand the school Online safety Rules. • I will use the computers, network, internet and other new technologies in a responsible way at all times. • I know that my network and Internet access is monitored.

Signed:	**Date:**

Parent's Consent for Web Publication of Work
I agree that my son/daughter's work may be electronically published.

Parent's Consent for Internet Access
I have read and understood the school online safety rules for my child to access the Internet in school. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

This agreement stands for the time the named child attends Kitwell School or until the demands of the Computing Curriculum (or technology) require it to be adapted.

Signed: **(Parent/guardian)**	**Date:**
Please print name:	