PINNER PARK INFANT & NURSERY SCHOOL

ACCEPTABLE USE of IT POLICY

It is generally agreed that there is no present or foreseeable future technical solution that can consistently guarantee the preclusion of pupils and staff from access to, or contact from, unwanted internet material. Neither can current technologies provide schools or a user with consistent safe use of the hardware or Computing systems. The protection of sensitive pupil, staff and school data is also a concern. The school will therefore implement and monitor the following policy to ensure appropriate, responsible and safe use by staff, pupils, parents and any other users of the school's computing systems.

Aims

The internet and other digital information and communication technologies are powerful tools which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work.

The school aims to continually develop, and keep up-to-date, the learning environment to provide a range of IT opportunities and tools, and to teach the skills needed to use these efficiently and safely. This will empower children to make relevant and safe choices, and to be flexible as they develop their personalised learning in line with the school's vision.

This Acceptable Use of IT Policy is intended to ensure:

- That staff and pupils are responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- That school IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- That all users are protected from potential risk in their use of IT in their everyday work;
- That staff have good access to IT to enhance their work and to enhance learning opportunities for children;
- That the General Data Protection Regulations is adhered to and any breaches are reported to appropriate bodies immediately;
- That staff agree to be responsible users.

Provision of IT in school

The school uses external providers to maintain and manage the IT systems and networks in school, and to ensure systems are in place to minimise the chances of users encountering or accessing undesirable material. They will also maintain the hardware and software within school.

Procedures

1. Evaluation of Internet content

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider (London Grid for Learning –LGfL) via the Achievement Leader for Computing or person designated by the Headteacher.
- The school will ensure the use of Internet derived materials by staff and pupils complies with copyright law; pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet derived material in their own work.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Staff will be trained to evaluate web materials and in ways of developing pupils' critical attitudes.

2. Management of email

- Pupils are provided with the ability to send and receive emails through the use of the school's Managed Learning Environment (MLE) – dBprimary. This is highly restricted (children can only send and receive emails from children in their own class/community) and closely monitored.
- Pupils must immediately tell a teacher if they receive an offensive email, either verbally or through the use of the whistle on the MLE.
- When communicating using emails pupils must not: reveal details of themselves or others such as address or telephone number; attach photographs / selfies / videos; arrange to meet anyone.
- Parents / carers take responsibility for the use of email at home.
- Staff are provided with an email account for their professional use (London Staff Mail) and it is made clear that personal emails should be through a separate account.
- The LGfL Staff Mail is a password protected email system that must be used to send and receive emails regarding school business but must adhere the GDPR. Staff must not use personal email accounts for school business (See Data Protection Policy) - the following exceptions can be applied:
    - Staff may send non-sensitive/non-confidential information to personal email accounts on logistical matters (e.g. arranging meetings, appointments, agendas).

3. Management of Pinner Park Infant and Nursery School's Website

- The point of contact on the website will be the school address, email and telephone number; staff or pupils' home information will not be published.
- Images that include pupils will be selected carefully and will not enable individual pupils to be identified, other than by personal facial recognition.
- Pupils' names will not generally be used on the web site other than in special circumstances where specific consent will be given in advance by their parents / carers.
- Information about the use of photographs on the school website is included in each child's Induction Pack on their entry to the school. This includes a form for parents to sign and return giving permission, or not, for the school to use images of their child (no names attached) on the website.
- The school uses external providers to design and to host the school website, however the Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

4. Social Networking and Use of Chat Rooms

- Pupils will not be allowed access to social networking sites except those that are part of an educational network or approved Learning Platform.
- Pupils must not reveal details of themselves or others such as address or telephone number, arrange to meet anyone or upload photos / selfies / video clips of themselves.
- Pupils will be taught the importance of using social networking and video sharing websites safely and responsibly when at home as part of the online safety curriculum (e.g. Facebook, Twitter Youtube, Instagram, Whatsapp); their online behaviour should not impact upon the school or its staff or pupils.
- All pupils will be taught the importance of reporting any concerns they have regarding social networking.
- Staff will use social networking sites with caution; they will take responsibility for ensuring the appropriate security settings of such sites and will not compromise their professional status or the school.
- Pupils will not be allowed access to public or unregulated chat rooms.

5. Management of emerging Computing systems and Internet applications

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones, personal tablets etc will not be used during lessons. The sending of abusive, threatening, defamatory, libellous or inappropriate text messages, sounds or images (still or moving) is forbidden.

6. The authorisation of Computing systems and Internet access

- Pupils and staff are provided with accounts for the school's computer network, the MLE and other home learning systems.
- Governors are provided with an account for the school's MLE, dBprimary.
- The school will keep a record of all staff and pupils who are given access to the school's computer network and the Internet. The record will be kept up-to-date, e.g. staff may leave and their permissions removed or a pupil's access be withdrawn.
- The school system has Bee Safe software installed, the school IT Provider's own software, to monitor pupil and staff use of the school's computing systems. The Provider, Beebug, make regular checks and send reports to the Headteacher, there is also a school portal where further monitoring can be run by the school if required. Warnings are given to staff of unacceptable use and information provided to senior staff with irrefutable evidence of misuse which can lead, at the least, to the withdrawal of access to the school's computing systems. If serious misuse is detected, they may be subject to disciplinary action and / or the LA or Police may be informed.

7. Risk Assessment

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable and / or is age-inappropriate for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the LA 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 are in place - Web filtering blocks banned sites and runs checks on the content of all sites and e-mails, blocking those where inappropriate material is identified.
- The Headteacher will ensure this policy is implemented and compliance is monitored through the school's IT Provider.

8. Management of Internet content filtering

- The school will work in partnership with LGfL to provide the safest possible access to the Internet and highest quality content filtering; the filtering strategy selected by LGfL will suit the age and curriculum requirements of the pupils.
- If staff or pupils discover unsuitable sites, the URL and content will be reported to LGfL by the person designated by the Headteacher.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal will be referred to LGfL and the Internet Watch Foundation (IWF).

9. Consultation of staff

- All staff must read, sign acceptance of and return a copy of the terms of the school's **Acceptable Use of IT Agreement**.

- All staff including teachers, Teaching Assistants and support staff will be provided with access to the Acceptable Use of IT Policy, and its importance will be explained.
- Staff should be aware that computer and Internet traffic will be monitored and traced to the individual user; discretion and professional conduct is essential; staff who operate monitoring procedures should be supervised by senior management.
- Staff development on safe and responsible Computing systems, Internet use and the Appropriate Use of Computing Systems Policy will be provided as required.

10. Computing system security (see also the school's **Data Protection Policy**)

- Sensitive data of any type will only be stored on the school's servers in the password protected or authorised access only areas.
- School laptops used by staff, which may be taken off site, are username/password protected. Staff will only save data temporarily on hard drives, uploading to the school servers as soon as possible and clearing it from the laptop hard drive. Staff will be advised to use encrypted pen drives for tighter security.
- Staff will ensure all their passwords are strong and reviewed regularly.
- The security and integrity of the school's computing systems will be regularly reviewed in conjunction with the school's IT Provider.
- Virus protection will be installed on all computers and updated regularly; all school laptops have **anti-virus and spyware software** installed on their hard disks which is updated when the laptop is connected up to the school system. Protection from viruses is achieved by using the industry standard anti-virus software from Sophos Ltd.; the school works in conjunction with its IT Provider on the installation and maintenance of this protective software. The Sophos console automatically updates every hour and is checked fortnightly by the IT provider.
- Personal and sensitive data sent over the Internet will be encrypted or otherwise secured (see the school's **Data Protection Policy**).
- Use of portable media such as USB devices will be reviewed; they may not be used in school without specific permission and only after a virus and spyware check has been carried out, and they must be encrypted / password protected if there is any sensitive data stored on it.
- Unapproved applications or executable files will not be allowed in users' work areas or emails.
- The Achievement Leader for Computing, along with the IT Provider, will ensure the capacity of the Computing systems expands in line with increased use.

11. Complaints procedure about Internet use

- The Headteacher is responsible for handling incidents.
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the Police must be contacted; early contact should be made to establish the legal position and discuss ways forward.
- Sanctions for misuse of the school's Computing systems include:
    - Child:
      - interview / counselling by their classteacher and/or the Headteacher/Deputy Headteacher;
      - informing parents, guardians or carers;
      - removal of Internet or computer access for a period.
    - Member of staff:
      - interview with Headteacher;
      - verbal or written warning;
      - withdrawal of rights and permissions to access school systems;
      - possible disciplinary action;

- involvement of LA and / or police.

12. Parental support

- Parents' attention will be drawn to this policy in newsletters and on the school website.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged; this may include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of Computing Systems will be made available to parents.
- Interested parents will be referred to organisations such as the government's Parent's Internet Safety pages http://www.direct.gov.uk/en/Parents/Yourchildshealthandsafety/Internetsafety/index.htm and NCH Action for Children http://www.actionforchildren.org.uk/ .

13. Search engine and inappropriate images

- When pupils or staff use a widely available search engine for images (e.g. Google) they may find inappropriate pictures. Some may be pornographic, some may offensive in their representation of various groups of people and some will be inappropriate when related to pupils' ages. Even with more filtering and 'safe search' options, there may be instances where pupils and/or staff will find inappropriate images.
  - Access to images will be restricted by using the 'safe search' option within widely available search engines, although this is not completely safe.
  - The school will use educational search engines such as Kids Yahoo http://kids.yahoo.com/ or information vetted through the LGfL.

14. Introduction of the 'Acceptable Use of IT Policy' to pupils

- Rules for Computing systems and Internet access will be posted in all rooms where computers are used.
- E-Safety procedures are shown on screen in a child friendly format as soon as children log-on to the Computing system.
- Pupils will only use computers and access the Computing systems under the direct supervision of staff.
- Pupils will be informed that computer and Internet use will be monitored.
- Instruction in responsible and safe use of Computing systems will precede access to them.
- The School's online safety curriculum will ensure all pupils understand the importance of appropriate use of Computing systems, through both Computing and PSHE lessons.

15. Safeguarding, Monitoring and Alerting Procedures

- The purpose of such procedures is to ensure that:
  - pupils remain as safe as possible;
  - pupils feel safe and schools can be more confident that their the pupils are safe;
  - staff use the IT resources safely and in a professional manner;
  - schools' Computing systems are not abused or compromised.
- The presence on the school's computer network, or portable computers provided to staff, of any unacceptable videos, sound recordings, images, emails, voice messages or texts should be immediately reported to a person designated by the Headteacher. If these files are of such concern (for example, they clearly involve minors) and their source and location indicate deliberate or knowing staff or pupil misuse of the system, the Headteacher (or the designated member of staff for child protection) must be informed, the computer shut down, securely isolated and the matter reported to the LA's Child Protection Officer without delay.
- If, however, the unacceptable images, emails or texts are judged to be the consequence of *accidental* or *unknowing* use of the system, these files should be immediately and permanently removed from the hard disks concerned. This should be carried out by a person designated by the Headteacher in the

presence of another person. If, however, the images, emails or texts clearly involve minors the computer must be shut down, securely isolated and the LA's Child Protection Officer must be informed immediately.

- To help the school monitor this aspect of Safeguarding the IT Provider uses Bee Safe, encrypted on Beebug's site, to monitor user's use of the computer system.
- This monitoring process is especially important when laptops / tablets are connected to the school's computer network, either by cable or wireless technology, and thus have access to the Internet. This connection to the network also enables the movement of files from the laptop to the network and/or the school's Managed Learning Environment (MLE) and vice versa. Only devices provided by the school will be connected to the school's internet / Wi-Fi. The school will not provide visitors or non-staff members of the school community with the school's Wi-Fi security code or give them access to the school computer system.

Additional processes

- The school's access to the Internet is filtered via the school's connection to LGfL and the Internet Content Filtering Tool (ICFT) is regularly updated with the latest definitions;
- A list of sites to which access is blocked at both school level and at service provider level is established and maintained by the school's Technical Support Provider and LGfL; this will enable sites that are judged to be beneficial for learning and teaching to be accessed more quickly;
- The school reserves the right to carry out (or have their IT Provider carry out) a selective search of the physical hard disks of servers, desktop PCs and staff laptops to monitor and review stored images.

School Governors

- Governors nominate a specific governor who has responsibility for Computing. Their responsibilities include working with the school on the following:
    - Considering the funding and training requirements to meet Computing targets needs set by either the school or the national agenda;
    - How the school might respond when offered gifts of free or significantly discounted computers;
    - Monitoring the performance of the school's technical support provider and how they work in partnership with the school to develop Computing;
    - Contribute to the:
        a) formulation and monitoring of the schools Computing curriculum policy;
        b) co-ordination of that plan across the curriculum;
        c) monitoring of the legal requirements for IT, e.g. legal licensing of software for which a log will be kept;
        d) monitoring of the development of Computing as a curriculum subject.
    - Monitoring the development and implementation of this policy with pupils and staff;
    - Consider how Computing (particularly the school's MLE) might be developed as a resource for governors;
    - Governors might also find the following web sites useful sources of further information:
      http://www.ukgovernors.org.uk/or
      http://community.tes.co.uk/forums/17.aspx
    - The LGfL has a section developed specifically for parents and carers: https://www.lgfl.net/online-safety/resource-centre?a=1 under Online Safety.

16. Rules for responsible Internet and computer network use for pupils

- Teachers will work with their class to discuss, establish and adhere to a set of Computing rules that the children feel they 'own' and can uphold. The Computing rules are as follows:
    - We keep our usernames and passwords secret;
    - We don't tell anybody our address or telephone number;

- We tell a grown-up if we see something that makes us unhappy;
- We only search the Internet when there is a grown-up in the room;
- We know that the school can check what we have been doing on the computer;
- We send and open emails together;
- We write polite and friendly messages to people we know;
- We stop and think before we click;
- We decide what is fact, fiction or opinion;
- We are careful when talking to online 'friends';
- We understand why we should not send personal information, including photographs of ourselves or our friends;
- We always ask before opening or downloading files;
- We know that we can talk to a grown-up in school if we are worried about something.

- Sanctions(will need interpretation to the children)
  - Violations of the rules may result in a temporary or permanent ban from computer network use.
  - Additional action may be added in line with existing practice on inappropriate language or behaviour.
  - Where applicable, police or local authorities may be involved.

17. Dealing with complaints about Computing systems or Internet use?

- Responsibility for handling incidents will be delegated to the Headteacher.
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the Police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
- Sanctions for misuse of the school's ICT systems include:
  - interview / counselling by senior staff;
  - informing parents or carers;
  - removal of Internet or computer access for a period;
  - suspension or dismissal.

Acknowledgements:- Stanburn Primary School.

This policy builds on Local Authority and government guidance.

Policy Schedule
Reviewed at: **Full Governing Body 31.3.10** **Full Governing Body: 24.05.12** **Full Governing Body: 30.3.17** **Reviewed and amended at:** **Governing Body Meeting: 17.5.18**
Next Review: **Governing Body Meeting – March 2020**

Related Documents

Code of Conduct
Data Protection Policy
Guidance on Photographs and Moving Images of Children
Privacy Notices
Records Management Policy and schedule

PINNER PARK INFANT & NURSERY SCHOOL
Acceptable Use of IT Policy (AUP): Staff agreement form

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform (dBprimary), software, equipment (including mobile phones and cameras) and systems.
The computer network plus school laptops, tablets etc, which are owned by the school, are made available to staff to carry out and enhance their professional activities (teaching, research, administration and management). All use (including Internet use) should be related to these activities or pupils' education. The school reserves the right to examine or delete any files that may be held on its computer network or portable computers. It is essential that staff realise that use of the school network, computers, laptops and tablets will be monitored.

I agree and understand that:
1. Use of school Computing systems for access to inappropriate or unlawful materials (pornographic, racist or offensive material), personal financial gain, gambling, political purposes, posting anonymous messages, forwarding chain letters or advertising is forbidden;

2. Installing software or hardware to any piece of school owned equipment must be agreed by the Headteacher / IT Leader / IT Provider (Beebug) and recorded in the asset management file;

3. Access is via my authorised username and password, which is not given to any other person, and no attempt to bypass the school's Internet filtering system will be made;

4. Any usernames and passwords provided by the school **must not** be disclosed to any other person, and my passwords must be strong and reviewed regularly;

5. I will be held accountable for any inappropriate use of the school's IT equipment for which I am responsible and if the laptop or tablet is taken home I will ensure that it is not misused;

6. Any electronic data concerning pupils or staff taken off the school premises must be stored only in the password protected area of the hard drive or on an encrypted USB drive assigned to me, must be used appropriately and must be wiped as soon as it has been used for its purpose;

7. School provided laptops used regularly at home must be brought into school from time to time to enable the anti-virus, anti-spyware, network and utilities software to be updated;

8. I am responsible for all emails sent and received (from whatever sources) and will ensure that all work related emails are sent through LGfL Staff Mail;

9. The copyright of materials must be respected and sources acknowledged when used;

10. Social networking sites (e.g. Facebook) and video sharing websites (e.g. YouTube) will be used with caution; I am responsible for ensuring the appropriate security settings of such sites (and 'friends' and groups) will not compromise my professional status or the school;

11. All use of school IT systems will be in compliance with the school's Appropriate Use of IT Policy and Data Protection Policy, copies of which I have access to;

12. All incidents of concern, breaches of regulations or loss of equipment or data **must** be reported immediately to a member of the Leadership Team.

User Signature

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 agree to abide by all the points above.

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

Full Name ..... (printed)

PINNER PARK INFANT & NURSERY SCHOOL

Data Confidentiality Agreement: Staff agreement form

For further information, see the school's Appropriate Use of IT Policy, Data Protection Policy and Computing Policy.

When accessing data staff will, at all times, comply with the Data Protection Act 2018. The use of the data will be consistent with the purpose for which the computing systems, MLE (dBprimary) and Management Information System (MIS) were constructed.
The data will be processed securely and not be subject to any unauthorised use or disclosure. Only authorised users will access the system and they will never share their login details with anyone else.
Staff with responsibility for managing and accessing personal data in the school's MIS from Capita SIMS or any other systems linked to them, are strongly advised to agree to the following.

As a member of staff who has access to sensitive personal data about the children and other staff colleagues, I agree and understand that:
a) the data will be used only for educational purposes and in the interests of the person to whom that data belongs, and not for any other purposes;
b) personal data will be shared only with those who need the information to discharge a statutory education function;
c) the management of usernames and passwords is the responsibility of the authorised SIMS system manager, the school's nominated USO Contacts and Atomwide Ltd;
d) care will be taken to protect any data that is printed or otherwise displayed;
e) procedures are in place to protect any data in transit; data is never taken out of the system in an unprotected / unencrypted form;
f) temporary data sets will be deleted as soon as possible.

User Signature

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 agree to abide by all the points above.

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

Full Name ..... (printed)

PINNER PARK INFANT & NURSERY SCHOOL

School Website

We would like to include a range of material on the website, including photographs. These would be of the school, displays and work by the children, and of the various activities and events that children are engaged in that make our school such a special place.

To comply with the Data Protection Act 2018, we need your permission before we can photograph or publish pictures on the website.

In using photographs for the website we:

- will not use the personal details of children or adults beside their photographic image on our website, although we may use class names eg '1LW planting seeds'.
- will not use a child's first name beside a photograph of them or a piece if their work without specific consent.
- may use group or class photographs with very general labels, such as 'A science lesson' or 'Making fruit smoothies'.
- will only use suitable images of pupils and staff.
- may display a range of work under a general heading with no names attached eg 'Minibeast paintings by 2MA'

We would appreciate being able to use photographs as they so clearly demonstrate the work of the school. You have already completed a photograph slip on the school's admission form, but as the website is something different, we are seeking permission for this separately.

Please fill in the form below and return it to school as soon as possible.

✂----------

Photographs for the School Website

Child's name …… Class ……

☐ I agree to my child's photograph being used on the school website – no names published

☐ I do not want my child's photograph to be used on the school website

Parent's/Carer's signature …… Date…….