North Hinksey C E Primary School

Online Policy

Values

We are a Church of England School and all our work is underpinned by core Christian values of faith, hope and love.

Vision

To provide a high quality, holistic education, enabling everyone to flourish and achieve through developing their intellectual, spiritual, physical and emotional wellbeing.

Aims

Create a safe, enjoyable and nurturing learning environment
Provide outstanding pastoral care for everyone
Value, encourage and equip every member of the school team in their respective roles
Create a culture of high expectations through all areas of school life
Create a motivating learning environment through inspirational teaching
Support all children to engage fully in their own learning and promote a love of learning
Encourage each child to develop self-confidence, practise care and respect for others
Welcome difference and celebrate all that we can learn from each other

This policy applies to all members of the school community including staff, pupils, volunteers, parents / carers and visitors who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

1) Head teacher and Senior Leaders

a) The Head teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online safety and Computing Co-ordinator.
b) The Head teacher and Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff as detailed in the 'Allegations of Abuse against staff' policy.
c) The Head teacher is responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
d) The Head teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
e) The Head teacher will receive regular monitoring reports from the Online Safety Co-ordinator.
f) The Head teacher receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.

g) Appropriate staff will be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
    i. sharing of personal data
    ii. access to illegal / inappropriate materials
    iii. inappropriate on-line contact with adults / strangers
    iv. potential or actual incidents of grooming
    v. cyber-bullying

2) Computing and Online Safety Coordinator:

a) Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies.
b) Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
c) Provides training and advice for staff.
d) Liaises with school technical staff
e) Meets with link safeguarding governor to discuss current issues and review incidents.
f) Attends relevant meetings of Governors.
g) Reports to Senior Leadership Team as necessary.

3) Teaching and Support Staff

a) Have an up to date awareness of online safety matters and of the current school online safety policy and practices.
b) Have read, understood and signed the Staff Acceptable Use Agreement.
c) Report any suspected misuse or problem to the Headteacher for investigation.
d) Ensure that all digital communications with parents / carers should be on a professional level and only carried out using their own school email address or the parent mail messaging system.
e) Should not have any digital communication with pupils.
f) Have a responsibility to ensure that the online safety curriculum is taught well and embedded in other aspects of the curriculum and activities.
g) Ensure that pupils understand and follow the online safety and acceptable use policies.
h) Ensure that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
i) Monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
j) 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.
k) Staff should act as good role models in their use of digital technologies the internet and mobile devices.

4) Technical staff

The Online safety and Computing Coordinator in conjunction with external technical staff are responsible for ensuring:

a) That the school's technical infrastructure is secure and is not open to misuse or malicious attack
b) That the school meets required online safety technical requirements and guidance
c) That users may only access the network and devices through a properly enforced password protection policy
d) That the external technical staff keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
e) That filtering and monitoring systems are implemented and updated as agreed in school

5) Pupils

a) Are responsible for using the school's digital technology systems in accordance with the Early Years/Key Stage 1 or Key Stage 2 Acceptable Use Policy and may face sanctions in line with those laid out in the Behaviour Policy which could result in their temporary or long term removal from using the technology. This also includes an understanding that their online behaviour outside of school may have an impact in school.
b) Have a good understanding the need to avoid plagiarism and uphold copyright regulations.
c) Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

d) Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that what they learn in school relates to their behaviour in and out of school.

6) Parents / Carers

a) Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about online safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:
    I. digital and video images taken at school events

7) Visitors

a) Community Users who access school systems as part of the wider school provision will be expected to read, sign and understand a staff Acceptable Use Agreement before being provided with access to school systems including devices, as well as internet.

Policy Statements

8) Education – Pupils

The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

a) A planned online safety curriculum will be provided as part of Computing / PHSE lessons and should be regularly revisited which will be reinforced within other whole school and class based activities such as assemblies.
b) Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.
c) Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
d) Pupils should be helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
e) In lessons where internet use is pre-planned, it is best practice that 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.
f) Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
g) It is accepted that from time to time, for good educational reasons, pupil may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff or online safety coordinator can temporarily remove those sites from the filtered list for the period of study.

9) Education – parents / carers

a) Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

b) The school will therefore seek to provide information and awareness to parents and carers through:
    i. Curriculum activities
    ii. Letters and, newsletters
    iii. Parents / Carers evenings
    iv. High profile events / campaigns eg Safer Internet Day

10) Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

a) A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
b) All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.
c) The Online safety Coordinator and Head teacher will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
d) This Online safety policy and its updates will be presented to and discussed by staff in staff meetings
e) The Online safety Coordinator will provide advice / guidance / training to individuals as required.
f) All visitors to school will be reminded not to use their mobile phones while children are present, communicated by the sign in the office.

11) Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure and network are as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

a) School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
b) There will be regular reviews and audits of the safety and security of school technical systems.
c) Servers, wireless systems and cabling must be securely located and physical access restricted.
d) All users will have clearly defined access rights to school technical systems and devices.
e) All users will be provided with a username and secure password by the designated member of technical staff who will keep/have access to an up to date record of these usernames and passwords. Users are responsible for the security of their username and password

f) The "master / administrator" passwords for the school ICT system, used by technical staff employed by the school is also be available to the Headteacher as necessary.
g) The school business manager is responsible for ensuring that software licence logs are accurate and up to date and that checks are made to reconcile the number of licences purchased against the number of software installations
h) Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the filtering provided. The filtering provider categorises all websites using keyword categorisation which the school then selects and filters all sites within the categories of; adult/sexually explicit, intimate apparel/swimwear, intolerance & hate, proxies/translators, proxy url rewriting, advertisement or pop-ups, alcohol & tobacco, criminal activity, gambling, hacking, illegal drugs, peer to peer, personals & dating, phising/online fraud, ringtones/mobile downloads, spam urls, spyware, tasteless & offensive, violence, weapons, virus worm infected, social networking, illegal file-sharing, suicide & self-harm.
i) All staff can request for websites to be added to the allowed list but first must discuss with the online safety coordinator who will liase with the headteacher to make a decision.
j) All staff should also report any concerns with websites that require adding to the banned list of websites.
k) Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
l) All staff must have express permission from the designated technical staff and/or the online safety coordinator before download executable files and installing programmes onto school devices.
m) All personal data should be sent using .sch.uk email address or using school registered data storage.

12) Use of digital and video images

a) Staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

b) Staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
c) In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be made public anywhere online.
d) Staff and volunteers are allowed to take digital images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
e) Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
f) Photographs published on the website, or elsewhere that include pupils will be selected carefully and parents will have provided prior agreement for these photos through the autumn pack.
g) Pupils' full names will not be used anywhere on a website or newsletter, particularly in association with photographs.

13) Data Protection

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

a) Fairly and lawfully processed
b) Processed for limited purposes
c) Adequate, relevant and not excessive
d) Accurate
e) Kept no longer than is necessary
f) Processed in accordance with the data subject's rights
g) Secure
h) Only transferred to others with adequate protection.

14) The school will ensure that:

a) It holds the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
b) Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
c) It has a Data Protection Policy.
d) It is registered as a Data Controller for the purposes of the Data Protection Act (DPA).
e) Data subjects have rights of access and there are clear procedures for this to be obtained which are detailed in the data protection policy.
f) All data is kept securely on site whilst in use, it is then archived securely off site at the end of each year and when the relevant time period has elapsed it is then securely destroyed.

15) Staff must ensure that they:

a) At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
b) 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.
c) Transfer data using encryption and secure password protected devices.

16) When personal data is stored on any portable computer system, memory stick or any other removable media:

a) The data must be encrypted and password protected .
b) The data must be securely deleted from the device, once it has been transferred or its use is complete.

Signed: ……..Head Teacher

Date: ……

Signed: ……Chair of Governors

Date: ……

Date of Policy:

Date to be reviewed: