St John's Highbury Vale CE Primary School

E-Safety Policy

St John's Highbury Vale CE Primary School Vision for Education:

"I can do all things through Christ who strengthens me."

Philippians 4:13

This can be lived out through our school moto,
'*every child, every opportunity, every day.*'

At the heart of our school vision is a desire for an authentic and life-giving relationship with one another and with God. We believe that it is through Christ who gives us the strength, all can achieve within a learning environment where every child is valued as a unique individual created in the image of God, and where teaching and learning is of a consistently high standard.

CONTENT

Rationale

Information and Communications Technology in the 21st Century is seen as a powerful tool and an essential resource that opens up new opportunities, which promote discussion, stimulate creativity and increase awareness of context to support effective learning and teaching. As well as playing an important role in the everyday lives of pupils and staff, both in school and at home, they have also been shown to raise educational standards and further pupils' achievement. Consequently, schools need to build in the use of these technologies in order to build up the resilience of each individual pupil whilst arming them with the skills to access life-long learning and employment.

Ofsted describes e-safety as a school's ability to protect and educate pupils and staff in their use of technology as well as having appropriate mechanisms in place to intervene and support any incident where appropriate. By working together, senior leaders, governors, staff, pupils and their families, can develop a clear strategy for e-safety that integrates safety and safeguarding effectively into the school's curriculum, and at home, to ensure that pupils have a strong understanding of how to keep themselves safe in light of technological developments.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. The breadth of e-safety issues are considerable and the ways in which these internet technologies can amplify the dangers and vulnerability our pupils and staff, both inside and outside of the classroom, include:

- Exposure to inappropriate, illegal, or harmful images/content, including unsuitable, non-age-appropriate videos/games
- Access to harmful lifestyle (e.g.self-harming) and hate websites
- Unmediated communication or contact leading to blackmailing, 'gifting', sexting or sharing/distributing personal images without an individual's consent or knowledge.
- Data Privacy and Security issues including identity theft, sharing passwords, gaining unauthorised access to/loss of/sharing of personal information and personal location.
- Content validation – inability to evaluate the accuracy, quality or the relevance of information on the internet
- Being cohersed into gangs or being radicalised
- Negative digital footprint and on-line reputation
- Health and well-being issues due to excessive use impacting on the individual's learning, and social and emotional development
- Copyright and plagiarism infringement
- Illegal downloads – video, music files and apps

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At St John's Highbury Vale C of E Primary School**,** we understand the responsibility to educate our pupils on E-Safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. As a result, this e-safety policy is used in conjunction with other relevant school policies (e.g. PHSE, Behaviour and Safeguarding policies).

Monitoring

This e-safety policy has been developed by:

- Executive Head Teacher
- Head of School
- Senior Leaders
- Teachers
- Support Staff
- Governing Body
- Data Protection Officer

Scope of the policy

Both this policy, and the Acceptable Use Agreement, applies to the school community, (including staff, governors, pupils, parents/carers, visitors and community users) who have access to and are users of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

The Education and Inspections Act 2006, empowers Head teachers, 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 cyber-bullying or other E-Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The Data Protection Act 2018, guides organisations in how they should protect and use individual's personal information. Therefore, the requirements of the act have been incorporated into this policy. The school acknowledges that balance needs to be struck in order to keep data appropriately secure whilst at the same time keeping systems and procedures functional and practical.

The school will deal with such incidents within this policy and associated policies and will, where known, inform parents / carers of incidents of inappropriate E-Safety behaviour that take place out of school. These will be logged on CPOMs.

Acceptable Internet Use Policy: Pupils

Rules to help keep the children and computer equipment of St John's Highbury Vale C of E Primary School safe:

- I will use my knowledge about E-Safety to guide me and keep me safe whenever, or wherever I am online.
- I will tell an adult if something makes on the internet makes me feel worried or uncomfortable.
- I take responsibility for my own use of all computing equipment and will use it safely, responsibly and within the law.
- I will only use the school's computing equipment for school work and not to upset or bully others, or to create a bad impression of my school.
- I will not access others people's files without their permission.
- I will not let anyone access my personal user account or give them my log in details.
- I will understand the school will check my computer files and monitor the websites I visit.
- I will respect copyright and I will not copy anyone's work and call it my own.
- I will not give my full name, any passwords, my home address, or my telephone number to anyone on the internet, or in any e-mail, nor arrange to meet anyone out of school.
- I will report unpleasant maternal to an adult immediately so that they can protect other children and myself.
- I will discuss internet safety issues with my parents/carers and uphold any rules for safe internet use in my home.

Signed by pupil: _____ Date: _____

Signed by parent/guardian: _____ Date: _____

Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school's Computing Lead.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body
- I understand that the email account given to me by the school is not a personal account but has been loaned for the duration of time I work for the school. Therefore, it is subject to monitoring and if required access by approved individuals.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- My passwords will be "strong" in nature, and include capitals, lower case, number, and symbol and be of least 8 characters long. If I suspect it has been compromised then I will change it immediately.
- I will ensure that I am the only one who uses my user Account and understand that anything undertaken while I am logged in, will be considered done by me.
- I will lock my computer screen whenever I leave it unattended.
- I will not autosave my password or log in details for any school systems, as this negates the effectiveness of the password.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- If I receive a suspicious email, I will report it before clicking on any links, downloading any attachments or entered my user details. When I report it, I will not forward the email but send a screen shot.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other social media link, to pupils.
- My personal social media accounts will not show a direct link with the school and I understand that whatever I post can be seen by parents, pupils or colleagues, therefore if I am identifiable content will be of a professional nature.
- I will only use the approved, secure e-mail system(s) for any school business and always check if I should be CC'ing Bcc'ing recipients and that the correct email address has been selected.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Executive Head, Head of School or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g., on a password secured laptop or a password protected document.
- I will transfer personal data by email securely e.g. using egress, or password protecting it. The password will be sent in a sperate email.
- I will not install any hardware or software without permission of the Head of School.
- I will consider if the communications I send breach confidentiality or the Data Protection Act, by asking "should the recipient view this information".
- I understand that I can cause a Data Protection breach by destroying or corrupting data and all data should be held in line with the School data retention schedule.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member and held in line with the school retention schedule.
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head of School.
- ➢ I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community' onto my own social media platforms.
- ➢ I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Executive Head or Head of School.
- ➢ I will respect copyright and intellectual property rights.
- ➢ I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.
- I will support and promote the school's E-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …….…….…… Date ……

Full Name ……..... (printed)

Job title ……

Roles and Responsibilities

The following section outlines the roles and responsibilities for E-Safety of individuals and groups within the school:

E-Safety Lead

The links between child protection and E-Safety are obvious. The lead on E-Safety will therefore be the Head of School:

- takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies / documents
- lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding
- be aware of procedures to be followed in the event of a serious online safety incident
- ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of E-Safety incidents and logs them
- is trained in E-Safety issues and be aware of the potential for serious child protection issues to arise from:
  - sharing of personal data
  - access to illegal / inappropriate materials
  - inappropriate on-line contact with adults / strangers
  - potential or actual incidents of grooming
  - cyber-bullying
- is deputised by the two Assistant Head teachers

Governors

Governors are responsible for: the approval of the E-Safety Policy; reviewing the effectiveness of the policy; ensuring that St John's Highbury Vale C of E Primary School has policies and practices in place to keep pupils and staff safe online; and supporting the school in encouraging parents and the wider community to become engaged in online safety activities. The E-Safety Governor is also the Link Governor for Safeguarding.

The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Lead
- regular monitoring of E-Safety incidents
- regular monitoring of filtering
- reporting to Governors

Computing Lead / Technical staff

The Computing Lead is responsible for ensuring:

- the delivery of the Computing curriculum, the progression in skills and evidence in relation to pupil achievement

The ICT Technician is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy
- that he/she keeps up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant
- that servers, wireless systems and cabling are securely located

---

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices
- they have read, understood and signed the school Staff Code of Conduct for Hounslow and the staff information booklet
- they report any suspected misuse or problem to the E-Safety Lead (Head of School)
- digital communications with students / pupils (email / Virtual Learning Environment (VLE)) are on a professional level
- E-Safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school E-Safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they model safe, responsible and professional behaviours in their own use of technology
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of E-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 are 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

- they are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Pupils

Pupils are responsible for using the school ICT systems in accordance with the Pupil Code of Conduct, which they and their parents will sign before being given access to school systems. Pupils need to:

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They will also know and understand school policies on the taking / use of images and on cyber-bullying.

- understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related in any way to the school

- they are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

- contribute to any 'pupil voice'/surveys that gathers information of their online experiences

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet /mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Code of Conduct

- reading, understanding and promoting the school's Pupil Acceptable Use Agreement with their child/ren

- consulting with the school if they have any concerns about their children's use of technology

- supporting the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images

- supporting the school in promoting online safety

- modelling safe, responsible and positive behaviours in their own use of technology.

Policy Statements

Education –pupils

E-safety education will be provided in the following ways:

- A planned E-Safety programme is provided as part of the computing curriculum for each class
- Key E-Safety messages are reinforced as part of a planned programme of assemblies, PHSE lessons, anti-bullying, E-Safety days/themes
- Pupils are taught to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- Through lesson planning that is age-appropriate and supports the learning objectives for specific curriculum areas
    - by reminding students about their responsibilities through the pupil Acceptable Use Agreement(s);
    - by ensuring staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright
    - by ensuring pupils only use school-approved systems and publish within appropriately secure/age-appropriate environments.

Education & Training – Staff

Training is offered as follows:

- formal E-Safety and training in Purplemash, Zoom and Google Classroom (home learning platform)
- induction for new staff to include E-Safety
- discussions by staff in staff/team meetings/INSET days
- provide, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever creating a digital footprint, which may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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:

- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they must recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- 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

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images must only be taken on school equipment.

- Care will be taken when taking digital / video images that staff and pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Pupils must not take, use, share, publish or distribute images of others without their permission. Staff should teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

- Photographs published on the website, or elsewhere that include staff and pupils will be selected carefully and will comply with good practice guidance on the use of such images.

- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Ipads and cameras will not be used for other purposes other than tracking and recording and uploading to tapestry.

Data Protection

Personal data including class lists etc. will be recorded, processed, transferred and made available according to the Data Protection Act 2018, which states that personal data must be (see data protection policy):

- Fairly and lawfully processed
- Processed 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.

Staff

Must ensure that they take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse at all times

- properly “log-off” at the end of any session in which they are using personal data
- only store personal data on secure devices (i.e. not on laptops).
- have approved virus and malware checking software on laptops etc.
- securely delete data from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

When using communication technologies the school considers the following as good practice:

- The official school email service (school comms) may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).

- Users must immediately report, to the e-safety Lead – in accordance with the school policy, the receipt of any digital communication that includes inappropriate material or makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

- Any digital communication between staff and pupils or parents / carers (email, chat, twitter, VLE etc) must be professional in tone and content and relevant to the educational purposes of the school.

- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They will also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

- Personal information will not be posted on the school website and only official email addresses will be used to identify members of staff.

Communication during school closure

Contact with parents/carers who require support with distance learning
Year group email access will be available for parents/carers to ask questions related to the curriculum and on-line learning, directly to class teachers.

Contact with parents/carers of children who are not accessing on-line learning
Class teachers will return a weekly class log to Phase Leaders to alert them to any children who are not engaging in on-line learning. These logs will be saved into the Phase Leader drive so that they are accessible to other senior staff in the event of a Phase Leader being unable to work.

Phase Leaders will make telephone contact with parents of children who are not active on-line to remind them of what is available and how their child can access this. These conversations will be logged and saved into the Phase Leader folder so that they are accessible to other senior staff in the event of a Phase Leader being unable to work.
Where telephone contact cannot be made an email will be sent from the admin email address

Keeping in touch with all parents/carers
Class staff will keep in touch with all families via phone calls or zoom. These calls will happen within a time frame set by the Head of School and will be focused on curriculum and home learning. Each family will receive one call during the allocated time period which may be followed up by an email from the year group email account if required.

Remote working
All teachers will be issued a school lap top and will be able to access the school system remotely.
Phase meetings/SLT will take place on google hangout.
Teachers will be allowed to pre-record videos that will be put into Google Classroom, once checked by the safety lead.
There will be no live streaming of any videos.

Unsuitable / inappropriate activities

Some internet activity, e.g. accessing child abuse images or distributing racist material is illegal and is obviously banned from school and all other ICT systems. Other activities, e.g. Cyber-bullying is banned and could lead to criminal prosecution. There are however a range of activities, which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

There are also uses of personal equipment outside of the school that could still lead to disciplinary action. The use of social networking sites in particular can lead to members of school staff compromising their professional standing. Staff are responsible for adjusting the settings on any site that they visit so that images or text cannot be viewed by pupils, or ex-pupils of the school. Where staff have friends who are parents of the school this is particularly important. Even with settings adjusted so that friends cannot pass communications on automatically to other friends of theirs, staff must be aware that it is still possible for such content to be circulated.

Incident Reporting

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. Illegal misuse will be reported to the police whereas the school will deal with incidents that involve inappropriate rather than illegal misuse. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's data protection officer. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are as follows:

- Head of School

All incidents will be dealt with as soon as possible through normal behaviour / disciplinary procedures, and members of the school community made aware that incidents have been dealt with.

Equal Opportunities

Pupils with Additional Needs

The school endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the schools' E-Safety rules.

However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Internet activities are planned and well managed for these pupils.

Prevent, Anti-radicalisation and Counter-Extreme Guidance

Ofsted states that all schools must ensure that pupils are safe from terrorist and extremist material when accessing the internet in school. Therefore, St John's Highbury Vale C of E Primary School, has ensured that it has suitable filtering in place, and as part of its wider safeguarding duties to prevent the possible radicalisation of vulnerable pupils, teaches its pupils about the risks of radicalisation in the same way that it teaches internet safety to protect pupils from other forms of harm and abuse.

Handling a sexting/nude selfie incident:

Following an issue there should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people
  When assessing the risks the following should be considered:
    - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
    - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
    - Are there any adults involved in the sharing of imagery?
    - What is the impact on the pupils involved?
    - Do the pupils involved have additional vulnerabilities?
    - Does the young person understand consent?
    - Has the young person taken part in this kind of activity before?
- If a referral should be made to the police and/or children's social care
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The imagery involves sexual acts and any pupil in the imagery is under 13
5. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply, then a school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support.

Review Procedure

There will be on-going opportunities for staff to discuss with the e-Safety coordinator any e-Safety issue that concerns them

There will be on-going opportunities for staff to discuss any issue of data security that concerns them

This policy will be reviewed every (24) months and consideration will be given to the implications for future whole school development planning

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way

This policy has been read, amended and approved by the staff, Head of School and Governors of St John's Highbury Vale C of E Primary School.