Blewbury Endowed C of E Primary School

'Shine your light and share it with the world!'

As a caring Church of England School community, we believe that the ethos of our school should be built on a foundation of core Christian Values. The following four core values reflect our school ethos and vision:

Community Appreciation Perseverance Forgiveness

E-Safety Policy

Chair of Governors: Ann Parham

Head of School:

Date: October 2021

Date of next review: October 2023

E-Safety Policy

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, governors) 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 cyber-bullying or other E Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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 E Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the E safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving information about E safety incidents and monitoring reports.

Headteachers and Leaders:

- The Head of School has a duty of care for ensuring the safety (including E safety) of members of the school community, though the day to day responsibility for E safety will be delegated to the Computing Lead
- School leaders should be aware of the procedures to be followed in the event of a serious E Safety allegation being made against a member of staff.
- The Head of school and the Senior Leadership Team are responsible for ensuring that the E Safety and computing Lead and other relevant staff receive suitable training to enable them to carry out their E Safety roles and to train other colleagues, as relevant.

Computing Leader:

- takes day to day responsibility for E Safety issues and has a leading role in establishing and reviewing the school E Safety policies / documents
- 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 school technical staff
- receives reports of E Safety incidents and creates a log of incidents to inform future E Safety developments
- reports to the Senior Leadership Team

Network Manager / Technical staff (123ICT):

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required E Safety technical requirements and any Local Authority Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep 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 the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leaders / Computing Lead for investigation and action
- that monitoring software / systems are implemented and updated as agreed in school policies

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 this and related policies
- they report any suspected misuse or problem to the Headteacher / Senior Leader; Computing Lead for investigation
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- E Safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the E Safety Policy and rules around acceptable use of technology
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they 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
- 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

Designated Safeguarding Lead

Should be trained in E Safety issues and be aware of the potential for serious child protection / safeguarding 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

Pupils:

- are responsible for using the school digital technology systems in line with instruction from school staff
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should 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 to their membership of the school

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. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local E Safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good E Safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

Policy Statements

Education – Pupils

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 E Safety is therefore an essential part of the school's E Safety provision. Children need the help and support of the school to recognise and avoid E Safety risks and build their resilience.

E Safety should be a focus in all areas of the curriculum and staff should reinforce E Safety messages across the curriculum. The E Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned E Safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key E Safety messages should be reinforced as part of a planned programme of assemblies

- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be helped to understand the need for pupil Acceptable Use Agreements and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – Parents / Carers

Parents and carers play an essential role in the education of their children and in the monitoring / regulation of their children's on-line behaviours. Parents may underestimate how often children come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

Education & Training – Staff / Volunteers

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

- A planned programme of formal E Safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive E Safety training as part of their induction programme, ensuring that they fully understand the school E Safety Policy and Acceptable Use arrangements.
- The Computing Lead will receive regular updates through attendance at external training and by reviewing guidance documents released by relevant organisations.
- The Computing Lead will provide advice / guidance / training to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

The school, along with 123ICT, will be responsible for ensuring that the school network is 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 E Safety responsibilities.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted

- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password.
- The administrator passwords for the school ICT system, used by the Network Manager must also be available to the Head of school or other nominated senior leader and kept in a secure place.
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Content lists are regularly updated and internet use is logged and regularly monitored.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the Network Manager.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g., trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies

Mobile technology devices may be provided by the school and might include: iPad, tablet, laptop that usually has the capability of utilising the school's wireless network. All users should understand that the primary purpose of the devices in a school context is educational.

Use of digital and video images

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, 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 cyberbullying 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.

- When using digital images, 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 e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / local press.

- Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims. These images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- 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.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Communications

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

- The official school email service may be regarded as safe and secure and is monitored. Staff 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 nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, blogs etc.) must be professional in tone and content**.** These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about E Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with in accordance with the school behaviour policy.