



E SAFETY POLICY (part of Child Protection Policy)

| | |
|--|-------------------------|
| Produced by: | Mrs A. Harding |
| Approved by Leadership Team on: | 03.10.2019 |
| Approved by Teaching & Personnel Standards Committee: | 16.10.2019 |
| Approved by Full Governing Body: Chair: Mrs B. Zeun Date: 06.11.2019 | Signature: _____ |
| Next Review Date: | November 2021* |

*Bi-annual review needed however Child Protection Policy requires annual renewal.

ALL POLICIES CAN BE VIEWED ON ONE DRIVE OR A COPY CAN BE REQUESTED BY EMAILING office@beaconsfield.school.

1.0 Development / Monitoring / Review of this Policy

1.1 This e-safety policy has been developed by a working group made up of:

- Headteacher
- Senior Leadership Team
- Staff – including Teachers, Support Staff, Technical staff
- Governors

2.0 Schedule for Development / Monitoring / Review

| | |
|---|--|
| This e-safety policy was approved by _____ | October 2019 |
| The implementation of this e-safety policy will be monitored by the: | <i>The Senior Leadership Team</i> |
| Monitoring will take place at regular intervals: | <i>Annually</i> |
| The <i>Governing Body</i> will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals: | <i>Annually</i> |
| The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: | November 2020 |
| Should serious e-safety incidents take place, the following external persons / agencies should be informed: | <i>Mr John Fletcher (Headteacher)</i> <i>Mrs Asha Harding</i> <i>External agencies</i> |

2.1 The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
 - students
 - parents / carers
 - staff

3.0 Scope of the Policy

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

3.2 The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students 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.

3.3 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.

4.0 Roles and Responsibilities

4.1 The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:-

4.2 Governors:

4.2.1 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 regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor (James McAvoy). The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs

4.3 Headteacher and Senior Leaders:

- The Headteacher 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 E-Safety Co-ordinator.
- The Headteacher and another member of the Senior Leadership 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 Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

4.4 E-Safety Coordinator:

- leads the e-safety committee
- 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 the Local Authority / relevant body
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

4.5 Network Manager / Technical staff:

4.5.1 The Network Manager / Technical Staff / Co-ordinator for ICT / Computing 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
- 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
- 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 / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; E-Safety Coordinator for investigation
- that monitoring software / systems are implemented and updated as agreed in school policies

4.6 Teaching and Support Staff

4.6.1 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 Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher / Senior Leader ; E-Safety Coordinator for investigation
- all digital communications with students / 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
- students understand and follow the e-safety and acceptable use policies
- students 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 students 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

4.7 Child Protection / Safeguarding Designated Person / Officer:

- should be 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

4.8 Students:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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.

4.9 Parents / Carers:

- 4.9.1 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 / VLE and information about national e-safety campaigns. 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
 - access to parents' sections of the website / VLE and on-line student records
 - their children's personal devices in the school

4.10 Community Users:

- 4.10.1 Community Users who access school systems / website / VLE as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

5.0 Policy Statements

5.1 Education – students

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

5.1.2 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 is provided as part of Computing whereby students complete an e-safety qualification. This curriculum will be regularly revisited.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Students 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.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students should be helped to understand the need for the student Acceptable Use Agreement 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 students 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 students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

5.2 Education – parents / carers

5.2.1 Many parents and carers have only a limited understanding of e-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.

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

- Letters, newsletters, web site, VLE
- Parents / Carers evening sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites e.g. www.saferinternet.org.uk/
<http://www.childnet.com/parents-and-carers>

5.3 Education – The Wider Community

5.3.1 The school will provide opportunities for local community groups to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide e-safety information for the wider community

5.4 Education & Training – Staff / Volunteers

5.4.1 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. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- 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 Agreements.
- The E-Safety Coordinator will receive regular updates through attendance at external training.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

5.5 Training – Governors

5.5.1 Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the County Council / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

5.6 Technical – infrastructure / equipment, filtering and monitoring

5.6.1. The school will be responsible for ensuring that the school infrastructure 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 by the Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every 3 months.
- 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. Illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / students etc.).
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach.
- 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. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- 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 extent of personal use that users (staff / students / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- 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.

5.7 Bring Your Own Device (BYOD)

- 5.7.1 The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by the school of users bringing their own technologies in order to provide a greater freedom of choice and usability.
- The school has a set of clear expectations and responsibilities for all users.
 - The school adheres to the Data Protection Act principles.
 - All users are provided with and accept the Acceptable Use Agreement.
 - All network systems are secure and access for users is differentiated.
 - Where possible these devices will be covered by the school’s normal filtering systems, while being used on the premises.
 - All users will use their username and password and keep this safe
 - Mandatory training is undertaken for all staff.
 - Students receive training and guidance on the use of personal devices.

- Regular audits and monitoring of usage will take place to ensure compliance.
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy.
- Any user leaving the school will follow the process outlined within the BYOD policy.

5.8 Use of digital and video images

5.8.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber 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:

- When using digital images, staff should inform and educate students 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.
- 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 is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.
- Staff and volunteers 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 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 students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students 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.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website
- Student's work can only be published with the permission of the student and parents or carers.

5.9 Data Protection

5.9.1 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018, which states that personal data must be:

- 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.

5.9.2 The school must ensure that:

- It will hold 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.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.
- It has a Data Protection Policy.
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA).
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs).
- Risk assessments are carried out.
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner’s Office.
- **The Data Protection officer (DPO) is Cecillie Gianneri (School Business Manager)**

5.9.3 Staff must ensure that they:

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

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

- The data must be encrypted and password protected.
- The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected).
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.