Belmont School
Online safety
(E-safety) Policy

Authorised: ……

(Headteacher)

Authorised: ……..…

(Chair of Governors)

Date Approved: 24-9-19

Date for Review: Autumn Term 2020/21

Online-Safety
Internet use is now an essential aspect of life, it pervades every activity that we undertake, and is increasing its hold. It is part of the statutory curriculum and is a necessary tool for staff and pupils. By design, it is insecure. Everyone in the school community has a personal responsibility to work towards keeping themselves and others safe online.

Infrastructure
- All aspects of the school IT systems are managed and reviewed by the IT Manager through a Managed Service Agreement with Bettridge School
- Internet access is a managed filtered service provided through South West Grid for learning (SWGfl). Virus protection purchased through SWGfl is installed on all compatible school devices and updates regularly.
- Security strategies will be periodically discussed within the IT steering group
- Physical and WiFi networks are secured – for instance through password protection
- A separated Guest network is in place for any visitors using IT on site

Filtering
- All internet access within the school is filtered through the use of standard filtering policies which are set by the SWGfL and custom filtering policies which are set by Belmont School. These are designed specifically with the safety of students in mind.
- Where access to a specific website is required by staff but not students, the website is un-filtered via the SWGfl custom filtering policies and then filtered from student users through our student specific internal proxy server.

Staff Responsibilities
- The IT Network and Development Manager regularly monitors internet access and brings any issues to the attention of the Leadership team who then take appropriate actions. This includes spot checking iPads for inappropriate content.
- The IT Network and Development Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Staff or administrative users will protect the school from computer virus attack or technical disruption by not downloading from the internet any programs or executable files other than by agreement with the school IT support staff.
- Staff will not purchase goods or direct services over the internet other than as specifically defined within the school finance policy
- All staff should at all times abide by the copyright laws in respect of documents and materials downloaded from the internet.
- All staff using school technology should have appropriate content only on their equipment. Staff should be aware that internet usage and technology devices content will be monitored.
- Staff using school technology (laptop/ iPad) off the school site, at home or elsewhere, still have to abide by this policy and the staff Acceptable Use Policy Agreement. Colleagues will be aware that the misuse of such devices for activity not agreed by the school may be breaking the law under the computer misuse Act 1990.

Misuse and complaints
- Any E-safety issues are logged and dated by the IT Network Manager and the Senior Leadership Team. Any action taken will be recorded. This includes information about the nature of the incident, who was involved and how it was dealt with. If the incident is of an illegal nature, the PC should be disconnected from the mains without shutting down first and the police and Local Authority Designated officer (LADO) informed. The log is reviewed to identify any trends and issues that may need addressing.
- If staff or students discover an unsuitable site, it will be reported to the IT support staff who will immediately ensure the website is filtered out and reported to the SWGfL.

- Complaints of internet misuse will be dealt with by a member of the Senior Leadership Team and any complaint about staff misuse will be referred to the Headteacher in accordance with the school's staff disciplinary procedures.
- Login passwords must not be shared with anyone. Users are provided with their own login passwords which can be used to monitor any action taken when logged on and every user is responsible for the action taken while there username is in use.
- Student's technology devices will be closely monitored and spot checked to ensure they are accessing appropriate content. (Please see students IT Student acceptable use policy).

Curriculum

Teaching:

- E-safety is mapped into our tutor times and is within PSCHE and computing curriculums. Students will be taught:
  - About the need to keep their username and passwords private and not to share this information with anyone
  - What internet use is acceptable and what is not and will be given clear guidelines for internet use.
  - About the effective use of internet research, including the skills of knowledge, location, retrieval and evaluation.
  - How to carry out safe internet searches, reducing the risk of accessing inappropriate material.
  - About the effective and acceptable use of the internet for web publishing.
  - To be aware of materials they read and shown how to validate information before accepting its accuracy.
  - About the safe use of the internet to support communications.
  - About what to do if they encounter a problem ad this includes how to report abuse.
  - About what to do if they are bullied over the internet (cyber or social media bullying).

Managing Internet Access for Teaching

- Students will be monitored when carrying out internet searches to ensure that they are accessing safe and appropriate material. Internet searches will be tested by an adult first to ensure that searches are safe.
- Primary pupils will be directly supervised accessing specific approved online material.
- The school will take all reasonable precautions to ensure that users access appropriate material. However it is not possible to guarantee that unsuitable materials will never appear on school technology, but action will be taken to prevent misuse or unsuitable access to content from happening again.

Training

- IT support staff and the curriculum computing co-ordinator will attend regular training in order to keep up- to- date with the latest recommendations
- There will be regular staff training regarding e-safety to ensure we are minimising potential risks.
- The school will communicate, support and advise parents in matters of e-safety, ensuring relevant information is being shared.
- All staff should acknowledge that they have read this policy.

Electronic Communications (e-mail)

- Students will only use approved e-mail on the school system
- Students will be supported using an e-mail. Offensive e-mails should be reported straight away to tutors/ middle managers/ safeguarding lead or members of the senior leadership team. All students' e-mails will be treated as public.
- Students must not reveal personal details of themselves or others in any online communication.
- Staff e-mails to outside organisations should be written using a professional voice (the same way as a letter would be written).
- The Belmont community must be polite and considerate online and report issues that are likely to cause offense to others.

- Teachers will support student's learning with regards to electronic communication
- Staff emails containing personal sensitive data should be sent confidentially using 'Egress' when sending to outside agencies
- Students are not allowed to have mobile phones with them on site. If brought into school they must be handed in to reception when they arrive and collected at the end of the day. Staff are not allowed to use personal phones in classrooms.
- Mobile phones (in any form) must not be used to take photographs/ videos of any student at any time.

Social Networking

- Belmont will block/ filter access to open social networking sites and will only give access to sites that are monitored and approved by the SWGfL.
- Tools including message boards, blogs and instant messaging will be used in safer, controlled learning sites which have been approved by the SWGfL.
- Students will be taught about the potential risks of social networking sites and what information should and should not be share don these sites.
- Staff should not provide information of their own, or another person/ pupil that could relate to Belmont School to any internet sites including all social media websites. Exceptions should be checked with the Headteacher.

Protecting personal data

- Personal data will be recorded, processed and transferred and made available according to the Data Protection Act 1998 and the General Data Protection Regulation 2015.

Acceptable use of Video Conferencing/ Skype

- A log will be kept of all video conference calls (including date, time, whom with and who else was present).
- Students must always be supervised by a member of staff when video conferencing
- Unsuitable content must be reported to the Designated Safeguarding Lead / Headteacher immediately.

Reporting

Incident Reporting – should anyone breach these policies for whatever reason – they should report breaches to a member of the Senior Leadership Team. If others are seen or suspected of operating in breach of these policies they must be reported immediately to the Designated Safeguarding Lead / Headteacher or the Deputy Designated Safeguarding Lead .

Monitoring and Review

This policy was drawn up by the Senior Leadership team in consultation with the IT Network and Development Manager and other members of the school staff .

Its implementation is seen as the responsibility of all staff. Its use and effectiveness will be supported and monitored by the Designated Safeguarding Lead with responsibility for Safeguarding in the school, on behalf of the Headteacher and Governors.

This policy will be reviewed annually and in line with any additional guidance issued.