Passed at resources committee 9.4.19 – R68 – 18/19

Bramley Vale E-Safety Policy

Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents - any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School - any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community - students, all staff, governing body and parents

Safeguarding is a serious matter. At Bramley Vale School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on a bi-annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Bramley Vale School website. Upon review all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use Policy. The Students Acceptable Use Policy is completed at school at the beginning of each school year. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place as such they will:

- Review this policy at least bi-annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents are appropriately dealt with and ensure the policy was effective in managing those incidents.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-Safety co-ordinator, as indicated below.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated e-Safety co-ordinator (currently Laura Fay) is engaging with the appropriate CPD in order to undertake the day to day duties. Andy Stoppard the previous e-safety co-ordinator has had CPD.
- All e-safety incidents are dealt with promptly and appropriately.

e-Safety Co-ordinator

The e-Safety co-ordinator will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher and governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.

- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or IT Technical Support.

- Make themselves aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher to decide on what reports may be appropriate for viewing.

IT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure.
- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Any e-safety technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Headteacher.
- Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters.
- The IT System Administrator password is to be changed on a regular basis.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any e-safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made), or in their absence to the Headteacher. If you are unsure, the matter is to be raised with the e-Safety Officer or the Headteacher to make a decision.

All Students

The boundaries of use of IT equipment and services in this school are given in the Student Acceptable Use Policy. Any deviation or misuse of IT equipment or services will be dealt with in accordance with the behaviour policy.

E-Safety is embedded into our curriculum. Students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents evenings, school newsletters and the school website the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the ICT in School Pupil Agreement before any access can be granted to school ICT equipment or services.

Technology

Bramley Vale School uses a range of devices including PC's, laptops and Ipads. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering - we use Exanet filtering that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites. Appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ICT Coordinator, e-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering - we use Sophos Puremessage software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption - All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

Passwords - all staff and students will be unable to access any device without a unique username and password. Staff and student passwords will change on a yearly basis or if there has been a compromise in data security. The ICT Coordinator and IT Support will be responsible for ensuring that passwords are changed.

Anti-Virus - All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as keydrives are to be scanned for viruses before use.

Internet - Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the Staff Acceptable Use Policy; students upon signing and returning their acceptance of the ICT in School Pupil Agreement. Older children are required to complete a Student Acceptable Use Form in September every year.

Email - All staff and students are provided with a secure school email address. Staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Photos and videos - All parents must sign a photo/video release slip when their child joins Bramley Vale. Non-return of the permission slip will not be assumed as acceptance. All photographs of children who left the school must be destroyed.

Social Networking - there are many social networking services available. Bramley Vale School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. A school Facebook page is set up and managed by the Headteacher.

Tapestry- is an online learning journal used by the Early Years Foundation Stage class teachers and support staff. All staff have separate login details, with a 12 character password and a pin number. Staff are permitted to use the learning journal outside of work to add to the child's profile. All photographs, videos and observations added are strictly confidential and only shared with the child's parent or carer. Parents have a login to access the journal but can only see their own child's information. For group observations, other parents can comment and see other children in the photograph, video or observation. Prior consent has been granted from parents when signing up to the journal. All parents and staff are not permitted to share media from Tapestry onto other social media platforms. We reserve the right to remove users. All staff observations have to be approved for parents to see them by the manager of the account, Laura Fay (Class Teacher).

In addition, the following is to be strictly adhered to:

- Permission slips must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy - should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any e-safety incident is to be brought to the immediate attention of the e-Safety co-ordinator, or in their absence the Headteacher. The e-Safety co-ordinator will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Bramley Vale School will have an annual programme of training which is suitable to the audience.

e-Safety for students is embedded into the curriculum. At Bramley Vale, we use the Purple Mash Scheme of Work which has e-safety embed within it. Whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The e-Safety co-ordinator is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Created on: 7th February 2017 by Andy Stoppard

Reviewed and updated on: 1st April 2019 by Laura Fay

Next review: April 2021