Bushey St James Trust

eSafety Policy

Last Reviewed:	July 2024	**Next Review:**	July 2026
Approved by:	Trust Board	**Date:**	11.7.24

Contents

The Trust e-Safety Policy has been written by the school, building on the Hertfordshire Grid for Learning Exemplar Policy (with acknowledgement to LGfL, SWGfL and Bristol City Council) and DfE guidance.

Rationale

ICT in the 21st Century is seen as an essential resource to support teaching and learning, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

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. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

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.

Across the Bushey St James Trust we understand the responsibility to educate our students on eSafety 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.

Both this Policy and the Acceptable Use Policy (for all staff, governors, visitors and students) are inclusive of both wired and wireless internet, technologies provided by the school (such as workstations, laptops, tablets, mobile phones, webcams, whiteboards, voting systems, digital video equipment, etc) and technologies owned by students and staff, but brought onto school premises (such as laptops, tablets, mobile phones, camera phones, and portable media players, etc).

Aims

As eSafety is an important aspect of strategic leadership within the school the Executive Principal and Governing Body have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

Senior Leaders and Governors are updated by the Executive Principal, Headteacher at Little Reddings Primary School and Hartsbourne Primary School, and all governors have an understanding of the issues and strategies at our schools in relation to local and national guidelines and advice.

This policy, supported by the Trust's acceptable use policy, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: anti-bullying, behaviour, child protection, complaints, code of conduct for employees and health and safety**.**

Practice

1.1 eSafety Skills Development for Staff

- our staff are made aware of eSafety issues within overall Child Protection sessions and briefing notes which summarise the school's e-safety policy
- all staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart Appendix A.)
- all staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

1.2 Managing the Schools' eSafety Messages

- we endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used
- the Acceptable Usage Policy will be introduced to the students at the start of each school year

1.3 eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the students on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- the school has a framework for teaching internet skills in ICT lessons and in specific assemblies and form/class time (ie CEOP)
- the school provides opportunities within a range of curriculum areas to teach about eSafety
- educating students on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum
- students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- students are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities
- students are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, through the 'Confide' button on all school computers or an organisation such as Childline/CEOP Report Abuse button, through the school website and learning platform.
- students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum

1.4 Password Security

Password security is essential for all users, particularly staff as they are able to access sensitive student data. Staff and students are expected to have secure passwords which are not shared with anyone. Staff and students are regularly reminded of the need for password security.

- all users read and agree to abide by an Acceptable Use Policy to demonstrate that they have understood the school's e-safety Policy
- users are provided with an individual network account which provides access to the school's network resources, email and Learning Platform. No individual network passwords are provided to students at both Little Reddings and Hartsbourne Primary Schools
- all students and staff are expected to use personal passwords and to keep them private
- students are not allowed to deliberately access on-line materials or files on the school network of other users
- all students and staff are expected to report to the IT Support team if they think their password may have been compromised or someone else may have become aware of their password
- staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS system (SIMS)**,** Learning Platform, including ensuring that passwords are not shared and are changed if they suspect that someone else is aware of their password.
- individual staff users must make sure that workstations are not left unattended unless locked. The default lockout time for the school network is 10 minutes of inactivity. While this can be adjusted by the administrator, users are advised to set this to a sensible limit which ensures the lockout time is still effective. When staff users launch data-sensitive applications such as the school's management information system (SIMS), a mandatory two minute lockout will come into effect
- when a user needs to leave the computer workstation unattended for a short period of time, they should initiate an immediate lock by pressing ❿ + L keys simultaneously
- in the Trust, all IT password policies are the responsibility of the IT Manager; all staff and students are expected to comply with the policies at all times. Students must set a password consisting of eight characters or more. Staff must set a password of eight characters or more and must change it at least every 180 days or at the request of a member of the IT department. .

1.5 Data Security

The accessing and appropriate use of school data is something that the Trust takes very seriously.

- staff are aware of their responsibility when accessing school data. Level of access is determined by the IT Manager in discussion with the Executive Principal/Headteacher, or appropriate member of the Senior Leadership Team
- any school mobile device that contains sensitive data will be encrypted
- staff users will give due consideration when logging into data-sensitive applications and websites to ensure that sensitive information is not inadvertently exposed or otherwise made available to those who do not have explicit permission to access it
- data containing student information may not be copied and/or removed from the school site, either electronically or using traditional paper-based methods, unless explicitly approved by a member of the Senior Leadership Team. Staff may only access student data off-site using approved remote access systems (Edulink, VPN, Chrome Remote Desktop). This applies to information held on school systems and information held by third parties as delegated by the school. It is the responsibility of the staff member to ensure data is kept secure when removed from the school site.

- the Trust acknowledges that there may be particular circumstances where child protection issues conflict with data protection guidance. In this instance advice should be sought from the Designated Safeguarding Lead (DSL)
- at least one full recent copy of school data will be held on-site, in addition critical data will be backed up to a remote location for the purpose of disaster recover. Additionally, a copy of the MIS and finance systems are backed up to a second off-site location to enable the school to restore core IT data services at alternative premises in the event of complete site contamination or irrecoverable damage to the school servers
- files stored in Google Drive that are deleted are accessible for 30 days from the point of deletion for restoration. Files that are not deleted have a full history of changes and can be reverted back to any point in the document's life at any time. It is up to the user to ensure that the correct permissions are given to collaborators to prevent changes to be overwritten and lost.
- personal devices may be connected to the student or staff wireless network at the discretion of the IT Support team
- users are aware that usage of all IT systems is monitored and logs recorded (including logging of keystrokes). These logs are accessible only to the IT Support Team. The logs may be randomly monitored to ensure compliance with Trust policy
- information logged pertaining to specific student use will be accessed and evidence provided to the relevant member of staff for the purpose of investigating contravention of any Trust and/or school rules or policy
- information logged pertaining to specific staff use will be accessed at the request of the Executive Principal/Headteacher and only divulged to the Executive Principal/Headteacher
- all staff must agree to abide by the terms of the E-Safety policy

1.6 Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the school internet connection is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- the Trust maintains students will have supervised access to Internet resources (where reasonable) through the school's wired and wireless internet technology
- all users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- all users must observe copyright of materials from electronic resources

1.7 Infrastucture

- the Bushey St James Trust has a monitoring solution provided by our internet filtering provider (Smoothwall). Learning, where web-based,is monitored and recorded
- School internet access is controlled through the Trust's web filtering service, currently provided by 'Smoothwall'. Smoothwall's Internet Filtering meets Ofsted's Online Safety Requirements.the Trust is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, General Data Protection Regulations (GDPR), The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- staff and students are aware that Trust based email and internet activity can be monitored and explored further using e-discovery tools, and understand that any evidence captured using e-discovery may be used as evidence in civil or criminal legal cases

- the Trust does not allow students access to internet logs
- the Trust uses management control tools for controlling and monitoring workstations. Teachers are trained to use this software in the classroom to ensure students are not distracted by unproductive activities, or expose themselves to unnecessary risk
- if staff or students discover an unsuitable site, the source and location of the material (eg website address, or location on the network) must be reported immediately to the IT Support team
- it is the responsibility of the school, and the IT Support Team, to ensure that anti-virus protection is installed and updated and to ensure relevant security patches are installed on all school computers
- students and staff using personal removable media (such as USB memory sticks) are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility to install or maintain virus protection on personal systems
- students and staff are not permitted to download programs or other executable files on school based technologies without seeking prior permission from the IT Support team
- if there are any issues related to viruses or anti-virus software, the IT Support team should be informed via the helpdesk (where available), or by visiting the IT Office in G block at Bushey Meads School
- the Trust does not restrict the usage of memory sticks and removable media from use, but all USB devices should be regularly scanned for viruses, and when used for transporting of confidential data, the USB device should be fully encrypted to minimise any risk of data leakage. The Trust recommends the use of Google Drive and Team Drives as the preferred method for storing and accessing data both in school and away from the school site. Removal media should only be used for storing non-confidential data where possible

1.8 Managing Web 2.0 technologies

The term "Web 2.0" refers to social and collaborative internet technologies; these include social networking sites (eg facebook, twitter, instagram), blogs (web logs), wikis (eg Wikipedia). If used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities.

However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- at present the Trust endeavours to deny access to social networking sites to students within school, except to Sixth Form students where it is appropriate and relevant to their chosen courses
- all students are advised to be cautious and to question the information given by others on sites, for example users not being who they say they are
- students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals

- students are encouraged to be wary about publishing specific and detailed private thoughts online
- students are asked to report any incidents of bullying to the school either by using the Confide button on school computers, via he CEOP Report Abuse website, or directly to a member of staff
- staff may only create blogs, wikis or other Web 2.0 spaces in order to communicate with students using the school's Learning Platform, Google Sites, or other systems approved by the Executive Principal/Headteacher. Staff are responsible for monitoring and moderating Web 2.0 spaces they create

2. Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, gaming devices, mobile and smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use.

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. The Trust chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

2.1 Personal Mobile Devices (including phones)

- the Trust allows staff to bring in personal mobile phones and devices for their own use. Only under exceptional circumstances does the school allow a member of staff to contact a student, parent or carer using their personal device
- Bushey Meads School students are allowed to bring personal mobile devices/phones to school but must not have them visible or use them for personal purposes within lesson time. At all times the device must be switched onto silent. Students are not permitted to bring mobile devices to school at both Little Reddings and Hartsbourne Primary Schools
- this technology may be used, however, for educational purposes where explicitly allowed by the class teacher. The device user, in this instance, must always ask the prior permission of the bill payer if using. Where possible students should use the school wireless internet connection when instructed to use a personal device
- the school is not responsible for the loss, damage or theft of any personal mobile device
- the sending of inappropriate content through any social medium between any member of the school community is not allowed and will result in further disciplinary action being taken
- permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device
- permission must be sought from the Site Manager before any personal devices (eg laptop/phone chargers) are connected to the school's electrical mains supply. The Site Manager will carry out or arrange the necessary portable appliance testing
- a minimum password of at least 4 digits on a mobile phone or tablet and 8 character password on a laptop or other device must be used
- the Trust remains the owner of all corporate data and has the capability to remotely move data including Email (Gmail), Google Drive and Google Calendar data through Mobile Device Management. By accessing data owned by the school through Google (GSuite) on a

mobile device, you consent to the Trust (as the Data Controller) to be able to remotely wipe corporate data from your device in the event of loss or theft. The Trust does not have the ability to wipe personal data, and it is the responsibility of the user to wipe this
- personal laptops should be encrypted when being used for work purposes, and when confidential data is held on the device directly. The Trust recommends use of the corporate VPN to securely access data relating to the Trust. This should be installed by the IT department

2.2 Trust Provided Mobile Devices (including phones)

- the sending of inappropriate content between any member of the school community is not allowed
- permission must be sought before any image or sound recordings are made on the devices of any member of the school community
- all software installed on Trust owned devices must be authorised by a member of the IT department
- the Trust reserves the right to remotely wipe all data from a corporate owned device as well as implementing further policies relating to password protection, app management, reporting and location information

Where the school provides mobile technologies such as phones, laptops and tablets for off site visits and trips, where possible only these devices should be used. If a personal device is used for school related activities, or any other reasonable circumstances, the data must always be removed from the device and copied onto the school network, under no circumstances should content remain on a personal device for longer than necessary.

If the device is lost and could contain confidential data relating to the school it must be reported to the Trust Data Protection Officer (DPO) so this can be logged as a potential breach. Further action may be taken at the discretion of the DPO.

3. Managing Email

Email is an essential means of communication for both staff and students within the Bushey St James Trust. In the context of the Trust, emails should not be considered private. Educationally, email can offer significant benefits including direct written contact between schools on different projects, be they staff based or student based, within school or internationally. We recognise that students need to understand how to style an email in relation to their age and good online etiquette.

- the Trust gives all students, staff, governors and trustees their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed
- the Trust does not allow students to access any email system than the account provided by the school in the interest of prevention of abuse of systems
- it is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all Trust business
- under no circumstances should staff contact students, parents or conduct any Trust or school business using personal email addresses. Governors and trustees are to only use the designated Trust email account for Trust business
- email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper. Email should be written in a formal

style, all stakeholders must act as a representative of the Trust in all written communications
- students may only use school approved accounts on the school system for educational purposes
- all email users are expected to adhere to the generally accepted rules of online etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission. All documents and attachments must be virus checked before opening
- students must immediately tell a member of staff if they receive an offensive email. Students are aware that they can contact the anti-bullying co-ordinators within each school to report such incidents
- staff must inform their line manager if they receive an offensive email
- students are introduced to email as part of ICT/Technology lessons when joining the school
- students agree and accept the schools acceptable use of ICT equipment as part of the home school agreement

4. Safe Use of Images

4.1 Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- unless the school is informed to the contrary it will be assumed appropriate digital images of students are permitted to be taken under the supervision of staff
- students and staff are permitted where appropriate for educational purposes, to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. All images must only be stored for as long as absolutely necessary, and must be deleted from the device once transferred onto a secure area on the school's computer network

4.2 Consent of Adults who Work within the Trust

- permission to use images of staff who work at the schools within the Trust will be sought on induction and a copy is located in the personnel file

4.3 Publishing Student's Images and Work

On a child's entry to the school, all parents and carers will be given the opportunity to opt-out of having their child's work/photos used in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents and carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Students' email and postal addresses will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

For further information relating to issues associated with School websites and the safe use of images in Hertfordshire schools, see

http://www.thegrid.org.uk/schoolweb/safety/index.shtml

http://www.thegrid.org.uk/info/csf/policies/index.shtml#images

4.4 Storage of Images

- images/ films of children are stored on the school's network and appropriate storage devices
- students and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Executive Principal/Headteacher
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network/ Learning Platform
- when students reach Year 9 they are able to provide self-consent to the use of their data including images on the school website, newsletter and any publications

5. Webcams and CCTV

The school uses CCTV for security and safety. Only the Executive Principal, Site Manager, Deputy Headteacher, and both Headteachers at Little Reddings and Hartsbourne Primary School are authorised to access recorded CCTV footage.

Live CCTV images are accessible to members of SLT (Senior Leadership Team) and various support staff. Notification of CCTV use is displayed at entrances to the school.

- we do not use publicly accessible webcams in school
- webcams in school are only ever used for specific learning purposes, and never using images of children or adults. Webcams are used for example for international classroom linked work via skype and facetime
- misuse of the webcam by any member of the school community will result in disciplinary action (as listed under the ' inappropriate materials' section of this document)

For further information relating to webcams and CCTV, please see
http://www.thegrid.org.uk/schoolweb/safety/webcams.shtml

6. Video Conferencing

- all students are supervised by a member of staff when video conferencing
- the school keeps a record of video conferences through computer/internet logs, including date, time and participants
- the school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences

- no part of any video conference is recorded in any medium without the written consent of those taking part

Additional points to consider:

- participants in conferences offered by 3rd party organisations may not be CRB checked
- conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

For further information and guidance relating to Video Conferencing, please see

http://www.thegrid.org.uk/learning/ict/technologies/videoconferencing/index.shtml

7. Misuse and Infringements

7.1 Complaints

Complaints relating to eSafety should be made to a member of the Senior Leadership Team and shall be raised with the appropriate external agency if required. Incidents should be logged and the Hertfordshire Flowcharts for Managing an eSafety Incident should be followed (see Appendix A). Please also see the school Complaints Policy for further information.

7.2 Inappropriate Material

- all users should report accidental access to inappropriate materials. The breach must be immediately reported to a member of the Senior Leadership Team for investigation
- deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator and, depending on the seriousness of the offence, investigation by the Executive Principal/Headteacher where disciplinary procedures will be followed, possibly leading to dismissal and involvement of police for very serious offences
- users are aware that school behavioural and disciplinary procedures will apply in the event of infringement on this policy. Students are reminded of expectations and sanctions in assemblies and lessons

8. Equal Opportunities

Students with Additional Needs

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

However, staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

9. Parental Involvement

We believe that it is essential for parents and carers to be fully involved with promoting eSafety both in and outside of school. We include guidance for parents and carers through induction and welcome evenings and we have produced helpful literature aimed at parents and carers.

- parents, carers and students can contribute to adjustments or reviews of the school eSafety policy by emailing the relevant school to which their child/children attend

- parents and carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school. When a child enters Year 9, under new legislation, a child can now provide their own consent for use of personal data
- parents and carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website) when their child joins the school
- in line with recommendations from county and the Trust's expectations, we request all parents and carers to observe age ratings for external websites, games and apps
- the Trust disseminates information to parents relating to eSafety where appropriate in the form of:
    - information, parent workshops and celebration evenings
    - website/Learning Platform postings and other relevant digital communication

10. Writing and Reviewing this Policy

10.1 Staff and Student Involvement in Creating this Policy

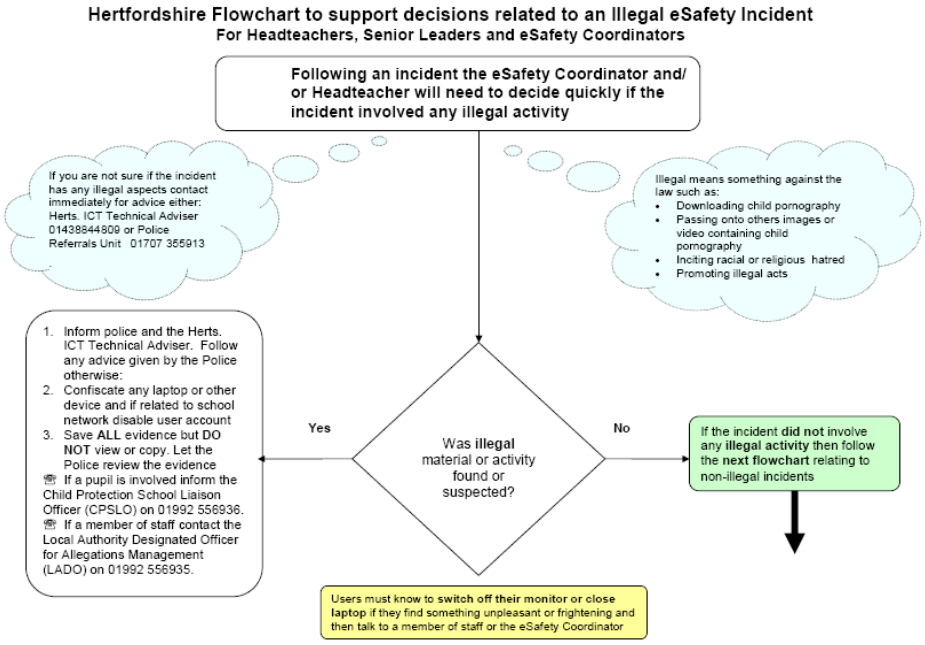
- Staff and students have been involved in making/reviewing the eSafety policy through consultation.

10.2 Monitoring & Review

This policy will be reviewed every 2 years and consideration 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.

Flowcharts for Managing an eSafety Incident



Current Legislation

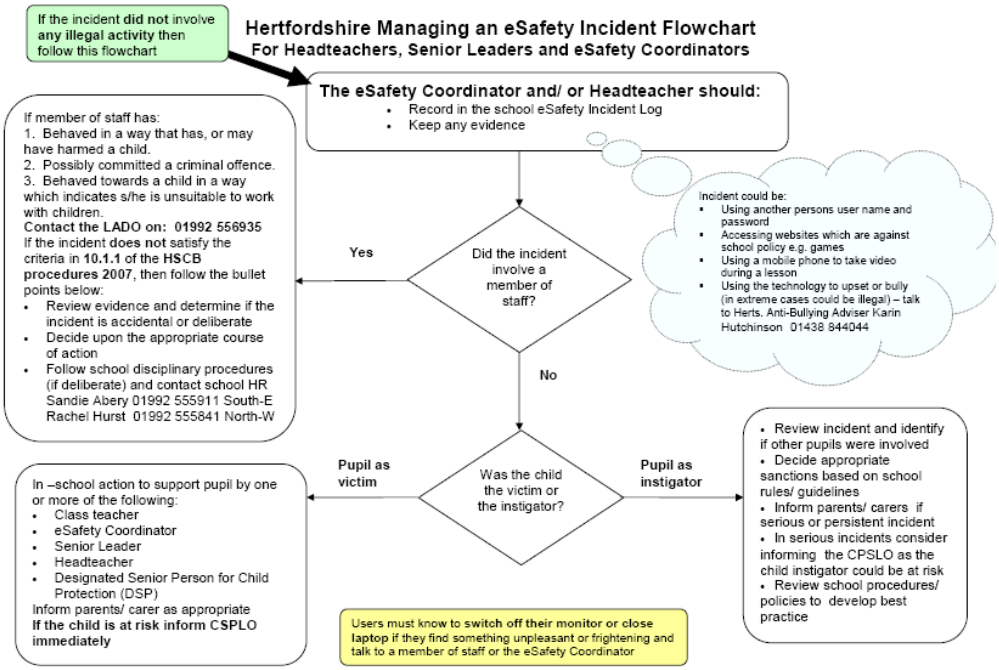
Acts relating to monitoring of staff email

Data Protection Act 1998 / General Data Protection Regulation (GDPR)
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm
https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure



communications are relevant to school activity or to investigate or detect unauthorised use of the network.

Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts relating to eSafety

Racial and Religious Hatred Act 2006
It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust.

Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.
For more information: www.teachernet.gov.uk

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of

the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.
Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Summary of Acceptable ICT Use by Staff, Governors and other Adults

For full details refer to the e-Safety Policy. This document is a summary of the main points of the policy for staff, governors and other adults.

The Bushey St James Trust provides IT resources for students, staff, Governors and Trustees for purposes of teaching, learning, administration and Governance. By using these resources you agree to abide by the terms set out in this document. This policy applies to the use of the school systems both on and beyond the school site.

Use of Facilities

1) You will not use the school systems to retrieve, store or transmit content that is abusive, offensive, threatening, or obscene.
2) You will not use the school systems for your own financial gain.
3) You will not attempt to compromise or disrupt the normal operation of the school systems.
4) You will not use the computers to play games unless you are given permission to do so.
5) You will respect the copyright and intellectual property rights of the work of others.

Equipment

1) You will not damage equipment, either intentionally or through negligence. The school will endeavour to keep all equipment in working order. If you find that a piece of equipment is not in working order, you should report it following the procedure set out in IT Support section of this policy. Unless you have been advised otherwise, you should not attempt to repair it yourself.
2) You will contribute to the security of all IT equipment, giving particular attention to mobile devices (eg laptops, cameras, tablets). You will reduce the risk of loss and theft by ensuring equipment is locked away at the end of the day, or returning it to the person or department issuing the loan.
3) You will ensure projectors, TVs and similar devices are turned off at the end of day to reduce energy waste and prolong the life of the equipment.

Monitoring

Your use of the school systems is fully monitored and audited; this may include the logging of keystrokes. Data logged will only be directly accessible to the IT Support team. Logs will be checked periodically to ensure compliance with school policy.

Members of staff may remotely monitor and control the computer you are using for the purpose of teaching and learning, technical support and to ensure compliance with school policy.

The school reserves the right to suspend your access to any or all of its IT systems without notice for the purpose of investigating an allegation or suspicion of misuse, misconduct, bullying, criminal activity or breach of school rules or policy.

IT Support

Support for the school IT systems is provided by the IT Support Team, situated in G block at Bushey Meads School. Students should report any problems to the teacher or other member of staff supervising their use of the equipment. Members of staff should use the web based IT Helpdesk system to contact the support team in the first instance, unless they are unable to (eg forgotten password), in which case they should telephone or visit the IT Support office.

Passwords

You will be responsible for keeping your account password secure by:

a) Changing it periodically.
b) Setting a password that is suitably complex so that it cannot be easily guessed by others.
c) Not disclosing your password to anyone, including your friends.
d) Not writing it down.

You may only access the school systems using your own account. If you become aware that someone else's password has been compromised, you will inform them without delay.
Your password should meet the following criteria:

Criteria	**Students**	**Standard Staff Account**
Minimum number of characters in password	Eight	Eight
Maximum password age*	None enforced, although it should be changed periodically	120 days
Password complexity requirements	None enforced, although a mix of numberic and alphanumeric characters (upper/lower case) is recommended	None enforced, although a mix of numberic and alphanumeric characters (upper/lower case) is recommended
Maximum number of consecutive characters	Two	Two

* When your account is about to expire, you will receive daily emails reminding you to change your password. Once the password had expired, the system will force you to change your password before you can logon to the network.

Data Security

1) You will take all reasonable precautions to ensure sensitive data is protected and not exposed to those who do not have permission to view it.
2) You will not remove or otherwise copy data pertaining to individual students from the school site. You may only remotely access such data using approved systems, including Learning Platform, Edulink, VPN.

Printing

Printing is expensive; ICT should encourage and enable paperless working. You will only print single copies of finished work. Print jobs consisting of multiple copies should be sent to a networked photocopier located in the professional learning area, reprographics, or a departmental photocopier. Alternatively you should make copies of single prints using a standard photocopier.

Email

a) All students, staff, Governors and Trustees are provided with a school/Trust email address, this is the only email system supported for use in school. School email should only be used to conduct school business.
b) Students are not allowed to use any email system, in school, other than the mailbox provided by the school.
c) Student, staff, Governor and Trustee users are allocated unlimited shared storage for email and Google drive storage.
d) Email is filtered by the school's service provider for viruses, spam, prohibited content and inappropriate language.
e) The IT Support team may access, intercept and read email in your school mailbox without notice for the purpose of investigating an allegation or suspicion of misuse, misconduct, bullying, criminal activity or any other breach of school policy.

Internet

The school's internet connection is provided and filtered by EXA Netwoks Ltd (exa.net.uk).
The school employs additional safeguarding protection provided by Smoothwall Ltd (uk.smoothwall.com) and internet filtering to ensure users receive age-appropriate content. You will not attempt to circumvent the school's web filtering. If you discover a website that is inappropriate, you should report it to the supervising member of staff, IT Support team or e-safety co-ordinator. While using collaborative technologies such as forums, wikis, blogs, Google Docs, Learning Platform, you will respect the views of others and not post or upload any content that could be offensive to others.

Personal Devices

You may connect personal devices such as laptops and mobile phones to the wireless network at the discretion of the BSJT IT Team. Furthermore if your device requires mains power, before plugging it in, you must seek permission from the Site Manager who will carry out the necessary portable appliance testing. It is the responsibility of the owner of the device to ensure it is free of viruses and malware, and ensure all relevant security patches are installed. Personal devices must be secured with a password of at least 8 characters in length, or a 4 digit pin/passcode. On a shared device, a separate user account must always be used for work purposes.

Remote Access

The school offers a number of services to enable remote teaching, learning and administration. All staff have access to the following **web services**: Google's web services for email and document collaboration http://www.google.com/a/busheymeads.org.uk.
Bushey Meads staff have access to the bms cloud (also referred to as the Learning Platform) https://bms.bsjt.cloud
Little Reddings staff have access to the lrs cloud
Hartsbourne staff have access to the hps cloud.

Bushey Meads Teaching staff are automatically given access to Edulink . Edulink enabled user accounts can remotely access elements of the school's management information system, including registers, marksheets, profiles and some student and staff information. A limited number of staff have access to a VPN (virtual private network) connection to the school. The VPN connection allows staff to access the same applications and resources as are available within school. VPN access requires authorisation by the IT Manager.

While using any of these remote access services, you should:

1) Contact the IT support team through this email address outside school should your password become compromised: it-support@busheymeads.org.uk
2) While logged into a password protected remote access service, the computer should not be left unattended. When you have finished using the remote access service, you should logout or disconnect as appropriate.
3) Keep any VPN configuration files for the (Smoothwall SSL VPN) secure, they should not be easily accessible to anyone other than the person who has been granted access. This file forms part of a multi-factor authentication system and contain a security key. You should also never disclose your username and password to anyone to prevent unauthorised connection to the secure encrypted VPN tunnel.
4) You should ensure any computers used to access remote services have relevant security systems in place including anti-virus software and all relevant security updates are installed. A minimum password must be set on the device of 8 characters in length, or 4 digit pin/passcode if using a smartphone or tablet device. Where possible a separate user account should also be used.

Summary of Acceptable ICT Use by Students

For full details refer to the e-Safety Policy. This document is a summary of the main points of the policy for students.

The schools within the Bushey St James Trust have excellent computer facilities that cost a lot of money to buy and maintain. As a student at a school within the Bushey St James Trust, you must respect these facilities and use them properly.

When you use them at school or from home, you are agreeing that you will:

Proper use

- never create, open, save or send anything that anybody else would find abusive, offensive, threatening, upsetting or obscene
- not do anything that would damage, delay or stop the school IT system working
- not play games unless you have been given permission to do so by a member of staff
- not copy or use the work of others without permission and when you do so with permission, you will show where you got the work from
- not try to use the IT system to make money
- report to a member of staff anyone who you believe is not using the school IT system properly

Equipment

- not damage equipment deliberately or through carelessness
- report to a member of staff any equipment that isn't working or is damaged. Sixth Form students can do this through the IT Help Desk
- not try to repair anything yourself
- help keep equipment safe by returning laptops, tablets and other mobile devices to the lockable cabinets, or to the person or department that issued the equipment
- help reduce energy waste by turning off projectors, TVs and similar equipment when they are no longer in use

Passwords

- never tell anybody else your password or let anybody else watch you typing it
- never write down your password
- change your password immediately if you think there is any chance that somebody else may know it
- never use anybody else's password
- tell someone if you know their password and advise them to change it
- not use passwords that are easily guessed by other people
- use a password that is at least eight characters long
- take responsibility for remembering your password

Printing

- only print if it is necessary as we are trying to help sustain the environment
- not print more than one copy of any piece of work (if you need more than one copy, you will have it photocopied)

Email

- only use your school email account when in school
- delete emails that don't need to be kept
- only email things connected with your work or with official school activities

Internet

- only use the internet with permission from a member of staff
- only use the internet for activities connected with your school work or with official school activities, unless you have been given permission to do so by a member of staff
- only use websites that are appropriate to and suitable for your work
- not try to get around any filters set by the school
- report to a member of staff any site that you come across and think shouldn't be available on the school system

Personal Devices

- you may connect your own laptop, mobile phone, iPod or similar device to the BMStudent wireless network at Bushey Meads only
- not plug any personal device into the school's electrical mains supply (eg laptop or phone charger) without first seeking permission from the Site Manager who must check the device to ensure it is safe.

Monitoring

You understand and accept that all your use of the school IT system is fully and closely monitored and that if you use it wrongly you will be punished and could lose your right to use it.

Data Security Addendum

Introduction
This addendum document encompasses all aspects of security surrounding confidential information and must be distributed to all Trust employees. All employees must read this document in its entirety and sign the form confirming they have read and fully understand this policy. This document will be reviewed and updated by Trustees and Governors as appropriate, on an annual basis or when relevant to include newly developed security standards into the policy and re-distributed to all employees and contractors where applicable.

Data Security Addendum
The Trust handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect the cardholder data, cardholder privacy, and to ensure compliance with various regulations, along with guarding the future of the organisation.

The Trust commits to respecting the privacy of all its customers and to protecting any customer data from outside parties. To this end management are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

Employees handling sensitive cardholder data should:

- handle Trust and cardholder information in a manner that fits with their sensitivity and classification
- limit personal use of the Trust information and telecommunication systems and ensure it doesn't interfere with your job performance
- the Trust reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose
- not use email, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal
- not disclose personnel information unless authorised
- protect sensitive cardholder information
- keep passwords and accounts secure
- request approval from management prior to establishing any new software or hardware, third party connections, etc
- not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval
- always leave desks clear of sensitive cardholder data and lock computer screens when unattended
- report information security incidents without delay to the individual responsible for incident response locally

We each have a responsibility for ensuring the Trust's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

Network Security
A high-level network diagram of the network is maintained and reviewed on a yearly basis. The network diagram provides a high level overview of the cardholder data environment (CDE), which at a minimum shows the connections in and out of the CDE. Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable should also be illustrated.

In addition, ASV (Approved Scanning Vendor) should be performed and completed by a PCI SSC Approved Scanning Vendor, where applicable. Evidence of these scans should be maintained for a period of 18 months.

Acceptable Use

The Trust is committed to protecting the employees, partners and the Trust from illegal or damaging actions, either knowingly or unknowingly by individuals.

- employees are responsible for exercising good judgment regarding the reasonableness of personal use
- employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data
- keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts
- all PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature
- all POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered
- the Trust maintains an inventory of all hardware equipment is regularly updated when devices are modified, added or decommissioned. A stocktake of devices will be periodically performed and devices inspected to identify any potential tampering or substitution of devices
- users should be trained in the ability to identify any suspicious behaviour where any tampering or substitution may be performed. Any suspicious behaviour will be reported accordingly
- information contained on portable computers is especially vulnerable, special care should be exercised
- postings by employees from a school email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Bushey St James Trust, unless posting is in the course of business duties
- employees must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code

Protect Stored Data

- all sensitive cardholder data stored and handled by the Trust and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by the Trust for business reasons must be discarded in a secure and irrecoverable manner
- if there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed
- PAN'S which are not protected as stated above should not be sent to the outside network via end user messaging technologies like chats, ICQ messenger etc

IT IS STRICTLY PROHIBITED TO STORE:

1) The contents of the payment card magnetic stripe (track data) on any media whatsoever.
2) The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
3) The PIN or the encrypted PIN Block under any circumstance.

Information Classification

Data and media containing data must always be labelled to indicate sensitivity level.

- confidential data might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to the Trust if disclosed or modified. Confidential data includes cardholder data
- internal use data might include information that the data owner feels should be protected to prevent unauthorized disclosure
- public data is information that may be freely disseminated

Access to the Sensitive Cardholder Data

All access to sensitive cardholder data should be controlled and authorised. Any job functions that require access to cardholder data should be clearly defined.

- any display of the card holder should be restricted at a minimum to the first 6 and the last 4 digits of the cardholder data
- access to sensitive cardholder information such as PAN's, personal information and business data is restricted to employees that have a legitimate need to view such information
- no other employees should have access to this confidential data unless they have a genuine business need
- if cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix A
- the Trust will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the for the cardholder data that the Service Provider possess
- the Trust will ensure that a there is an established process, including proper due diligence is in place, before engaging with a Service provider
- the Trust will have a process in place to monitor the PCI DSS compliance status of the Service provider

Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc
- media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals
- visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information
- procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. "Employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants who are "resident" on school sites. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to physically enter the premises for a short duration, usually not more than one day
- a list of devices that accept payment card data should be maintained
    - the list should include make, model and location of the device
    - the list should have the serial number or a unique identifier of the device
    - the list should be updated when devices are added, removed or relocated
- POS devices surfaces are periodically inspected to detect tampering or substitution

- personnel using the devices should be trained and aware of handling the POS devices
- personnel using the devices should verify the identity of and any third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices
- personnel using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the appropriate personnel
- strict control is maintained over the external or internal distribution of any media containing card holder data and has to be approved by management
- strict control is maintained over the storage and accessibility of media
- all computer that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use

Protect Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- card holder data (PAN, track data, etc.) must never be sent over the internet via email, instant chat or any other end user technologies
- if there is a business justification to send cardholder data via email or by any other mode then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, SSL, TLS, IPSEC, etc.)
- the transportation of media containing sensitive cardholder data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location

Disposal of Stored Data

- all data must be securely disposed of when no longer required by the Trust, regardless of the media or application type on which it is stored
- an automatic process must exist to permanently delete on-line data, when no longer required
- all hard copies of cardholder data must be manually destroyed when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner
- the Trust will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed
- the Trust will have documented procedures for the destruction of electronic media. These will require:
    - all cardholder data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media
    - if secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion
- all cardholder information awaiting destruction must be held in lockable storage containers clearly marked “To Be Shredded” - access to these containers must be restricted

Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into Trust practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- review handling procedures for sensitive information and hold periodic security awareness

meetings to incorporate these procedures into day to day company practice
- distribute this data security addendum to all Trust employees to read. It is required that all employees confirm that they understand the content of this document by signing the acknowledgement form
- all employees that handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with the Company
- all third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS)
- company security policies must be reviewed annually and updated as needed

Credit Card (PCI) Security Incident Response Plan

The Trust PCI Security Incident Response Team (PCI Response Team) is comprised of the Executive Principal, Headteacher, Finance Manager, Bursar and IT Manager. The Trust PCI security incident response plan is as follows:

1. Each department must report an incident to the Information Security Officer (preferably) or to another member of the PCI Response Team.
2. That member of the team receiving the report will advise the PCI Response Team of the incident.
3. The PCI Response Team will investigate the incident and assist the potentially compromised department in limiting the exposure of cardholder data and in mitigating the risks associated with the incident.
4. The PCI Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary.
5. The PCI Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.

The Trust PCI Security Incident Response Team:

a) Executive Principal – Jeremy Turner (BSJT)
b) Rachael Coombs – Finance Manager (BSJT)
c) Rebecca Tregear – Headteacher (Little Reddings Primary School)
d) Kathy Wong – Bursar (Little Reddings Primary School)
e) IT Manager (BSJT)

Information Security PCI Incident Response Procedures

- a department that reasonably believes it may have an account breach, or a breach of cardholder information or of systems related to the PCI environment in general, must inform the Trust PCI Incident Response Team. After being notified of a compromise, the PCI Response Team, along with other designated staff, will implement the PCI Incident Response Plan to assist and augment departments' response plans

Incident Response Notification

Escalation – First Level:

a) Finance Manager
b) Bursar
c) IT Manager

Escalation – Second Level:

a) Executive Principal
b) Headteacher

External Contacts (as needed)
a) Merchant Provider Card Brands
b) Internet Service Provider (if applicable)
c) Internet Service Provider of Intruder (if applicable)

Communication Carriers (local and long distance)
a) Business Partners
b) Insurance Carrier
c) External Response Team as applicable (CERT Coordination Center 1, etc)
Law Enforcement Agencies as applicable inn local jurisdiction

In response to a systems compromise, the PCI Response Team and designees will:
1. Ensure compromised system/s is isolated on/from the network.
2. Gather, review and analyse the logs and related information from various central and local safeguards and security controls
3. Conduct appropriate forensic analysis of compromised system.
4. Contact internal and external departments and entities as appropriate.
5. Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.
6. Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.

The credit card companies have individually specific requirements that the Response Team must address in reporting suspected or confirmed breaches of cardholder data. See below for these requirements.

Incident Response notifications to various card schemes
1. In the event of a suspected security breach, alert the information security officer or your line manager immediately.
2. The security officer will carry out an initial investigation of the suspected security breach.
3. Upon confirmation that a security breach has occurred, the security officer will alert management and begin informing all relevant parties that may be affected by the compromise.

VISA Steps
If the data security compromise involves credit card account numbers, implement the following procedure:
1. Shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.
2. Alert all affected parties and authorities such as the Merchant Bank (your Bank), Visa Fraud Control, and the law enforcement.
3. Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.

For more Information visit:
http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_ compromised.html

Visa Incident Report Template

This report must be provided to VISA within 14 days after initial report of incident to VISA. The following report content and standards must be followed when completing the incident report. Incident report must be securely distributed to VISA and Merchant Bank. Visa will classify the report as "VISA Secret"*.

I. Executive Summary
   a. Include overview of the incident
   b. Include RISK Level(High, Medium, Low)
   c. Determine if compromise has been contained
II. Background
III. Initial Analysis
IV. Investigative Procedures
   a. Include forensic tools used during investigation
V. Findings
   a. Number of accounts at risk, identify those stores and compromised
   b. Type of account information at risk
   c. Identify ALL systems analyzed. Include the following:
      - Domain Name System (DNS) names
      - Internet Protocol (IP) addresses
      - Operating System (OS) version
      - Function of system(s)
   d. Identify ALL compromised systems. Include the following:
      - DNS names
      - IP addresses
      - OS version
      - Function of System(s)
   e. Timeframe of compromise
   f. Any data exported by intruder
   g. Establish how and source of compromise
   h. Check all potential database locations to ensure that no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments, data on software engineers' machines, etc.)
   i. If applicable, review VisaNet endpoint security and determine risk

VI. Compromised Entity Action
VII. Recommendations
VIII. Contact(s) at entity and security assessor performing investigation

* This classification applies to the most sensitive business information, which is intended for use within VISA. Its unauthorized disclosure could seriously and adversely impact VISA, its employees, member banks, business partners, and/or the Brand.

MasterCard Steps:

I. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.
II. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured email to compromised_account_team@mastercard.com.
III. Provide the MasterCard Merchant Fraud Control Department with a complete list of all

known compromised account numbers.

IV. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).
V. Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
VI. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
VII. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs.
2. Distribute the account number data to its respective issuers.

Employees of the company will be expected to report to the security officer for any security related issues. The role of the security officer is to effectively communicate all security policies and procedures to employees within the company and contractors. In addition to this, the security officer will oversee the scheduling of security training sessions, monitor and enforce the security policies outlined in both this document and at the training sessions and finally, oversee the implantation of the incident response plan in the event of a sensitive data compromise.

Discover Card Steps

I. Within 24 hours of an account compromise event, notify Discover Fraud Prevention at (800) 347-3102
II. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
III. Prepare a list of all known compromised account numbers
IV. Obtain additional specific requirements from Discover Card

American Express Steps

I. Within 24 hours of an account compromise event, notify American Express Merchant Services at (800) 528-5200 in the U.S.
II. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
III. Prepare a list of all known compromised account numbers Obtain additional specific requirements from American Express

Transfer of Sensitive Information Policy

- all third-party companies providing critical services to the Trust must provide an agreed Service Level Agreement
- all third-party companies providing hosting facilities must comply with the Company's Physical Security and Access Control Policy
- all third-party companies which have access to Card Holder information must:

    1. Adhere to the PCI DSS security requirements.
    2. Acknowledge their responsibility for securing the Card Holder data.

3. Acknowledge that the Card Holder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.
4. Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.
5. Provide full cooperation and access to conduct a thorough security review after a security intrusion by a Payment Card industry representative, or a Payment Card industry approved third party.

User Access Management

- access to the Trust's systems is controlled through a formal user registration process beginning with a formal notification from HR or from a line manager
- each user is identified by a unique username so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out
- there is a standard level of access; other services can be accessed when specifically authorized by HR/line management
- the job function of the user decides the level of access the employee has to cardholder data
- a request for service must be made in writing (email or hard copy) by the newcomer's line manager or by HR. The request is free format, but must state:

  Name of person making request;
  Job title of the newcomers and workgroup;
  Start date;
  Services required (default services are: MS Office, Google Apps and mail, SIMS and Internet access)

- each user will be asked to read the e-safety policy and asked to sign a form indicating that they understand the conditions of access
- access to all school systems is provided by IT and can only be started after proper procedures are completed
- as soon as an individual leaves the Trust's employment, all his/her system logons must be immediately revoked
- as part of the employee termination process HR (or line managers in the case of contractors) will inform IT operations of all leavers and their date of leaving

Access Control Policy

- access Control systems are in place to protect the interests of all users of the Trust computer systems by providing a safe, secure and readily accessible environment in which to work
- the Trust will provide all employees and other users with the information they need to carry out their responsibilities in an as effective and efficient manner as possible
- generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient other controls on access are in place
- the allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner and IT Services. Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality
- access rights will be accorded following the principles of least privilege and need to know

- every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent
- users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification
- users are obliged to report instances of non-compliance to the IT Manager
- access to IT resources and services will be given through the provision of a unique Active Directory account and complex password
- no access to any IT resources and services will be provided without prior authentication and authorization of a user's Windows Active Directory account
- password issuing, strength requirements, changing and control will be managed through formal processes. Password length, complexity and expiration times will be controlled through Windows Active Directory Group Policy Objects
- access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing
- users are expected to become familiar with and abide by the school and Trust policies, standards and guidelines for appropriate and acceptable usage of the networks and systems
- access for remote users shall be subject to authorization by IT Services and be provided in accordance with the e-safety policy this data security addendum. No uncontrolled external access shall be permitted to any network device or networked system
- access to data is variously and appropriately controlled according to the data classification levels described in the data security addendum
- access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks and other methods as necessary
- a formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users' access rights. The review shall be logged and IT Services shall sign off the review to give authority for users' continued access rights

Agreement to Comply With Data Security

_____

Employee Name (printed)

_____

Department

I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to the company by third parties such as customers, will not be disclosed to unauthorised persons.

At the end of my employment or contract with the company, I agree to return all information to which I have had access as a result of my position.

I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal manager who is the designated information owner.

I have access to a copy of the Information Security Policies, I have read and understand these policies, and I understand how it impacts my job.

As a condition of continued employment, I agree to abide by the policies and other requirements found in the company security policy.

I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information security policies to the designated security officer.

_____

Employee Signature

_____

Date

List of Service Providers

Name of Service Provider	Contact Details	Services Provided	PCI DSS Compliant	PCI DSS Validation Date
Worldpay	0870 366 1233	Online card payments	Yes	