E-Safety Policy

Person responsible	e-Safety Co-ordinator
Last update	November 2016
Frequency of Review	Annual
Date of last review by Governors	June 2017
Date of next review by Governors	June 2018

Contents

1. Introduction and Overview

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Bute House Preparatory School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Bute House Preparatory School.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies, and to monitor their own standards and practice.
- Set clear expectations of behaviour and codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language); and substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online [internet or gaming])

- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

Ref: Ofsted (April 2014)

This policy applies to all members of Bute House Preparatory School (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of Bute House Preparatory School

The Education and Inspections Act 2006 empowers Heads to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school s*ite and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other E-Safety incidents covered by this policy, which may take place outside of school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Bute House Preparatory will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate E-Safety behaviour that take place out of school.

Roles and responsibilities

Role	Key Responsibilities
Head	• To take overall responsibility for e-safety provision • To ensure the school uses an approved, filtered internet service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious E-Safety incident • To have half-termly monitoring meetings with the E-Safety Co-ordinator
Bursar	• To take overall responsibility for data and data security

Role	Key Responsibilities
E-Safety Co-ordinator and Designated Safeguarding Person (DSP)	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school E-Safety Policy • Promotes an awareness and commitment to e-safeguarding throughout the school community • Ensures that e-safety education is embedded across the curriculum • Liaises with school ICT/Computing technical staff • Communicates regularly with SLT and the designated E-Safety Governor to discuss current issues and review incident logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident • To ensure that the e-safety incident log is kept up to date • Facilitates training and advice for all staff • Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: ▪ sharing of personal data ▪ access to illegal / inappropriate materials ▪ inappropriate on-line contact with adults / strangers ▪ potential or actual incidents of grooming ▪ cyber-bullying and use of social media
Governors	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the Governor/s will include regular review with the E-Safety Co-ordinator (including e-safety incident logs)
ICT Leader	• To oversee the delivery of the e-safety element of the Computing curriculum

Role	Key Responsibilities
	• To liaise with the E-Safety Coordinator regularly
Network Manager/technician	• To report any e-safety related issues that arise, to the E-Safety Coordinator • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are changed annually • To ensure that provision exists for virus and security threats (e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices • Ensures the school's policy on web filtering is applied and updated on a regular basis • Keeps up to date with the school's E-Safety Policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • The use of the school network/website/remote access/email is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Co-ordinator or Head for investigation • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster • Keep up-to-date documentation of the school's e-security and technical procedures • Ensure that all data held on pupils is adequately protected
School Secretary	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology, including, extra-curricular activities if relevant

Role	Key Responsibilities
	• To ensure that pupils are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the school's E-Safety Policy and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement as stated in the Information and Security policy • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the E-Safety Coordinator • To maintain an awareness of current e-safety issues and guidance (e.g. through CPD) • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc. • Ensure that the use of internet derived materials comply with copyright law
Pupils	• Read, understand, sign and adhere to the Acceptable Use Policy (AUP) which is sent to all pupils, annually, in September • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • Understand the importance of reporting abuse, misuse or access to inappropriate materials • Know what action to take if they or someone they know feels worried or vulnerable when using online technology • Know and understand school policy on the use of mobile phones, digital cameras and hand held devices • Know and understand school policy on taking and using images, and on cyber-bullying

Role	Key Responsibilities
	• Understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school • Take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home
Parents/carers	• Read and understand the school Pupil Acceptable Use Agreement, which will be sent home at the beginning of each new academic year • Support the school in promoting e-safety and endorse the Pupils' Acceptable Use Agreement which includes use of the internet and the school's use of photographic and video images • Access the school website in accordance with the relevant school Acceptable Use Agreement. • Consult with the school if they have any concerns about their children's use of technology
External groups	• Any external individual/organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website and saved on Teacherlink
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

Handling complaints

- The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by tutor/Head of Year/E-Safety Coordinator/Head;
- informing parents or carers;
- removal of internet or computer access for a period, [which could ultimately prevent access to files held on the system]

- Referral to Police.
- The E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head.
- Complaints of cyberbullying are dealt with in accordance with our **Anti-Bullying Policy**. Complaints related to child protection are dealt with in accordance with our **Safeguarding (Child Protection) Policy**.

Review and Monitoring

The E-Safety Policy is referenced from within other school policies: ICT and Computing policy, Child Protection policy, Anti-Bullying policy, Information and Security policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies.

- The school has an E-Safety Coordinator who will be responsible for document ownership, review and updates.
- The E-Safety Policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- The E-Safety Policy has been written by the school E-Safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school E-Safety Policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Pupil e-safety curriculum

This school

1 Has a clear, progressive e-safety education programme as part of the Computing curriculum/PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:

    - to STOP and THINK before they CLICK

2 to develop a range of strategies to evaluate and verify information before accepting its accuracy;

3 to be aware that the author of a website/page may have a particular bias or purpose and to develop skills to recognise what that may be;

4 to know how to narrow down or refine a search;

5 [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;

6 to understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;

7 to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;

8 to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;

9 to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;

10 to understand why they must not post pictures or videos of others without their permission;

11 to know not to download any files – such as music files - without permission;

12 to have strategies for dealing with receipt of inappropriate materials;

13 [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;

14 to understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.

15 to know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or CEOP.

16 to encourage pupils, who use the internet and social media, to be aware of the online risks associated with extremism, radicalisation and terrorism and therefore adjust their behaviours in order to reduce risks and build resilience (see **Safeguarding Policy** for details)

- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an Acceptable Use Policy which every student will sign at the beginning of each academic year
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons. For example, locking workstations when away from their computer, following correct personal mobile phone use guidelines, etc.

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming

Staff and governor training

Bute House…

- ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- makes regular training available to staff on e-safety issues and the school's e-safety education program;
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the E-Safety Policy and the school's Acceptable Use Policies.
- ensures all staff are familiar with and understand the E-Safety Disclosure Procedure

Parent awareness and training

Bute House runs a rolling programme of advice, guidance and training for parents, including:

- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear.
- Information leaflets; school newsletters; the school web site.
- Talks, presentations and practical advice sessions held at school.
- Suggestions for safe internet use at home.
- Provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy (AUP) which they will be expected to sign before being given access to school systems;
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences;

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school;
- will be expected to know and understand school policies on the use of personal mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking of and use of images.

Staff:

- are responsible for reading the school's E-Safety Policy and using the school ICT systems accordingly, including the use of personal mobile phones and hand held devices.

Pupils:

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers:

- should provide consent for pupils to use the internet, as well as other technologies, as part of the E-Safety Acceptable Use Agreement form at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse
- should support the school's adherence to regulatory e-safety requirements, including not uploading or sharing videos and/or photographs, on personal mobile phones or devices, of pupils other than their own children without permission of that child's parent/s
- should minimise the use of personal mobile phones and/or devices on school premises when in the presence of pupils at the school.

Incident Management

In this school:

- searches and web addresses are monitored and the IT technicians will alert senior staff where there are concerns and prevent further access when new sites that are unblocked are found;
- there is strict monitoring and application of the E-Safety Policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions;
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (e.g. the local authority, CEOP, UK Safer Internet Centre helpline) in dealing with e-safety issues;

- monitoring and reporting of e-safety incidents takes place and contributes to developments in policy and practice in e-safety within the school;
- parents/carers are specifically informed of e-safety incidents involving young people for whom they are responsible;
- the Police will be contacted if staff or pupils receive online communication that we consider is particularly disturbing or breaks the law;
- pupils' are able to report any e-safety concerns by accessing the 'Report It' button, which can be found at the footer of the school website.

4. Managing the ICT infrastructure

Passwords - see **ICT Policy** and **Information Security Policy** for details

E-mail - see **ICT Policy** and **Information Security Policy** for details

School website – see **Information Security Policy** for details

Social networking - see **Information Security Policy** for details

Video Conferencing - see **Information Security Policy** for details

CCTV - see **Information Security Policy** for details

5. Equipment and Digital Content

Personal mobile phones and mobile devices

- Designated areas for personal mobile use are situated in the setting (e.g. Staff Room). The areas where personal mobile phones should never be used are: toilets, bathrooms and changing areas.
- Personal mobile phones brought into school are entirely at the staff member, students' & parents' or visitors own risk. Bute House accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Staff members may use their personal mobile phones during school break times but never in the presence of children and preferably in the Staff Room. All visitors are requested to turn off or keep their phones on silent and ensure they remain out of sight of any children until they leave the premises. Visitors to the EYFS must give their phone to the member of staff in charge so that it can be locked away in compliance with Safeguarding regulations.
- The recording, taking and sharing of images, video and audio on any personal mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Head. All mobile phone use is to be open to scrutiny and the Head is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

- Bute House reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the School Office's telephone. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permission to use their phone other than their break times.

Students' use of personal devices

17 Bute House strongly advises that student mobile phones should not be brought into school.

18 Bute House accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety. This is applicable to Year 6 pupils only if making their own way to and from school.

19 Student mobile phones which are brought into school must be turned off (not placed on silent), handed in to the school office and locked away/stored out of sight. They must remain turned off and out of sight until the end of the day (this includes extra-curricular activities).

20 If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office and parents will be informed.

21 If a pupil needs to contact her parents or carers, they will be allowed to use a school phone. Parents should not contact their child via their mobile phone during the school day, but to contact the school office.

22 Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be given guidance and advice about safe and appropriate use of mobile phones and personally-owned devices, and will be made aware of boundaries and consequences.

23 Students must turn off 3G and 4G if bringing a device into school, e.g. a kindle.

24 Cyber-bullying by pupils. Via texts and emails, will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures.

Staff use of personal devices

- Staff are not permitted to use their personal mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or

personally-owned devices must not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Social Media

Social media is an increasingly influential part of life particularly for young people. It has been identified as an important tool in the sharing of extreme material and extremist groups are actively using social media to inform, share propaganda, radicalise and recruit for their cause. Social media safeguarding is an important element of protecting young people from extremist narratives and *Prevent* can play an active part in this process.

In this school:

25 Social networking sites will be blocked using suitable filtering systems to block inappropriate content, including extremist content where possible.

26 Parents and pupils will be provided with information on the safe use of the internet, through assemblies, workshops, talks and regular publications.

27 Where staff, students or visitors find unblocked extremist content they must report it to the E-Safety co-ordinator, Alice Charteris, or in her absence a senior member of staff.

The Prevent Duty (see also Safeguarding Policy)

28 We ensure that children are safe, as far as possible, from terrorist and extremist material when accessing the internet in school.

29 Suitable filtering is in place to ensure that children are safe from terrorist and extremist material when accessing the internet in school.

30 Pupils' will be equipped to stay safe online, both in school and outside of school.

31 Internet safety will be integral to school's Computing curriculum and is also embedded in PSHE and RE.

32 All staff are aware of the risks posed by online activity of extremist and terrorist groups, and know how to deal with it accordingly.

33 Arrangements to respond to pupils who may be targeted or influenced to participate in radicalism or extremism is of a high priority.

34 The Acceptable Use Policy (AUP) for staff, pupils and parents, and visitors, refers to preventing radicalisation and related extremist content.

35 To report any online terrorist related material visit: www.gov.uk/report-terrorism (see **Child Protection Policy** for more details)

Digital images and video

- Under the Data Protection Act 1988, at the start of each academic year, parental consent to the taking and use of photographs and videos will be updated for each pupil.
- When using photographic images of pupils on the School Website, they can be named. However, we do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published material outside of the website.
- Staff sign the school's Acceptable Use Policy (AUP) and this includes a clause on the use of mobile phones/ personal equipment for taking pictures of pupils.
- Only school cameras or school mobile phones can be used to take photographs of pupils
- Photographs are stored on computers which are password protected.
- In their e-safety education programme, pupils are taught about how images can be manipulated and are also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their Computing scheme of work.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make personal information, public.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.
- Parents' are allowed to take photos or videos of their children at school events for their own personal use. They must not upload them onto social media sites (if they have other children in them), without the permission of that child's parents.
- Other visitors to school (e.g. theatre groups or workshop providers) are not to photograph or film pupils during a school activity without the parents' permission
-

Asset disposal - see **Information Security Policy** for details

Details of all school-owned hardware will be recorded in a hardware inventory.

Details of all school-owned software will be recorded in a software inventory.

All redundant equipment that may have held personal data will have the storage media forensically wiped if sending to third party companies. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.