DOMINUS MAGISTER LUDI NOSTRI

STANBOROUGH SCHOOL

1919

A Policy and Guidelines for e-Safety

Lorraine Dixon Headteacher	Berton Samuel Chair of Governors

Approved/issue	February 2017	**Locations**	J Drive Appendix to School Handbook Website Headteacher's PA
Review Cycle	Annual		
Next review due	February 2018	**Circulation details**	Governors All staff Parents via website

Table of Contents

Definition of Terms

School: Stanborough Secondary School, including the Boarding School, International Stanborough School

Headteacher: Headteacher of the School

Pupils, Students: Pupils who attend the School

Staff: Any member of the staff employed by the School in either a teaching or non-teaching role, members of the Governing Body and Volunteers working within the School

1. Introduction

1.1 Stanborough School is a caring community founded upon Christian values and, as such, the well-being of each of its members is a prime concern.

1.2 Information and Communication Technology (ICT) has transformed the process of teaching and learning in the School. It is a crucial component of every academic subject, and is also taught as a subject in its own right. All pupils are taught how to research on the internet and to evaluate sources. They are instructed in the importance of evaluating the intellectual integrity of different sites, and why some apparently authoritative sites need to be treated with caution.

1.3 ICT and the communications revolution provide unrivalled opportunities for enhanced learning, but these new technologies can put young people at risk within and outside of the School. Some of the dangers they may face include:

- Unauthorised access to/loss of/sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The sharing/distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication/contact with others, including strangers;
- Cyber-bullying;
- Access to illegal, harmful or inappropriate images or other content and/or access to unsuitable video/internet games;
- An inability to evaluate the quality, accuracy and relevance of information on the internet;
- Plagiarism and copyright infringement;
- Illegal downloading of music or video files;
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-Safety Policy is used in conjunction with other School Policies including:

- Child Protection Policy
- Anti-bullying Policy
- Acceptable Use Policies
- Behaviour Management Policies for School.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

Pupils are therefore taught how to stay safe in this environment and how to mitigate risk, including identity theft, bullying, harassment, grooming, stalking and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment.

1.4 When using the Internet to enter or share information it is important that we consider what data we are making available and how this can be viewed by others. Most social networking sites have privacy settings which can and should be used to limit the audience who can access this information.

1.5 The Data Protection Act of 1998 was brought in to protect the rights and privacy of individuals and to ensure that data about them was not processed without their knowledge where possible. It covers data which is held in electronic formats.

2. Child Protection

2.1 The School recognises that internet safety is a child protection and general safeguarding issue. The Designated Senior Lead and the IT Manager have been trained in safety issues involved with the misuse of the internet and other mobile electronic devices. They work to promote a culture of responsible use of technology that is consistent with the ethos of the School. All of the Staff, especially those with pastoral responsibilities, receive training in e-safety issues.

2.2 The school has a programme on e-safety which ensures that all year groups in the School are educated, in an age-appropriate way, in the risks and reasons why they need to behave responsibly online. The Headteacher is responsible for overseeing the School.

3. Scope of the Policy

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

3.2 The Education and Inspections Act 2006 empowers Headteacher to such extent as is reasonable, to regulate the behaviour of pupils when they are off the School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the School, but is linked to membership of the School.

3.3 The School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/careers of incidents of inappropriate e-safety behaviour that take place out of school.

4. Roles and Responsibilities

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

4.1 Governors

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. The Safeguarding Governor has one meeting per term with the e-Safety Coordinator, where e-safety incident logs are monitored, and subsequently makes a report to the Full Governors' Committee each term.

4.2 Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the School community, though the day-to-day responsibility for e-safety will be delegated to the e-Safety Coordinator.
- The Headteacher is responsible for ensuring that the e-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in School who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The School Leadership Team will receive regular monitoring reports from the e-Safety Coordinator.
- The Headteacher and Assistants Heads should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (see flow chart on

dealing with e-safety incidents – included in Appendix 1 – "Responding to incidents of misuse" and relevant HR/disciplinary procedures).

4.3 E-Safety Coordinator

The e-Safety Coordinator:

- takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the School e-safety policy/ documents;
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- provides/organises training and advice for staff on e-safety matters;
- liaises with School ICT technical staff;
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- meets termly with the Safeguarding Governor to discuss current issues and review incident logs; reports regularly to the School Leadership Team.

4.4 IT Manager and Technical Staff

The IT Manager and ICT Assistants are responsible for ensuring:

- that the School's technical infrastructure is secure and is not open to misuse or malicious attack;
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed;
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant;
- that the use of the network/internet/ remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the e-Safety Coordinator/Assistant Head/Senior Teacher for investigation/ action/sanction;
- that monitoring software/systems are implemented and updated as agreed in School policies.

4.5 Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current School e-Safety Policy and practices;
- they have read, understood and signed the School Staff Acceptable Use Policy (AUP);
- they report any suspected misuse or problem to the Assistant Head/Senior Teacher for investigation/action/sanction;
- all digital communications with Pupils/parents/careers should be on a professional level and only carried out using official school systems;
- e-safety issues are embedded in all aspects of the curriculum and other activities;
- pupils understand and follow the e-safety and acceptable use policies;
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor ICT activity in lessons, extra-curricular and extended school activities;
- they are 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;
- in lessons where internet use is pre-planned Pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

4.6 Designated Senior Lead

The Designated Senior Lead should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data;
- access to illegal/inappropriate materials;
- inappropriate online contact with adults/strangers;
- potential or actual incidents of grooming;
- cyber-bullying.

4.7 Pupils

Pupils:

- are responsible for using the School ICT systems in accordance with the Pupil Acceptable Use Policy, which they are expected to sign before being given access to School systems;
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying;
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realize that the School's e-Safety Policy covers their actions out of school, if related to their membership of the school.

4.8 Parents/Guardians

Parents/Guardians play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Parents and guardians should ensure that Pupils only access social networking sites in accordance with the published age restrictions of such sites. Parents are also responsible for monitoring their children's internet use and for ensuring that their children are not involved in any incidents of cyber-bullying.

It is recognised that not all parents and careers may feel equipped to protect their son or daughter when they use electronic equipment at home hence the School organises occasions and age-appropriate information evenings for parents/guardians when a specialist offers advice about the potential hazards of this exploding technology, and the practical steps that parents/guardians can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm.

The School seeks to work closely with parents and guardians in promoting a culture of e-safety. The School will always contact parents/guardians if there are any worries about a child or young person's behaviour in this area, and parents/guardians are encouraged to share any worries with us.

Parents and guardians will be encouraged to support the School in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events;
- their children's personal devices in the school.

5. Policy Statements

5.1 Education – Pupils

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

e-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of ICT/PSHE and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside of school;
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and pastoral activities;
- Pupils will be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information;
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Pupils will be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside of school;
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

5.2 Education – Parents/Guardians

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/ regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational divide" (Byron Report).

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

- Specific Parent Information Sessions;
- Letters, newsletters, website.

5.3 Education and Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. It is expected that some staff will identify e-safety as a training need within their personal appraisal process;
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements;
- The e-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations;
- This e-Safety policy and its updates will be presented to and discussed by staff in staff/ INSET days;
- The e-Safety Coordinator will provide advice/guidance/training to individuals as required.

5.4 Training – Governors

Governors will be offered e-safety training through participation in School training/ information sessions for Staff or parents.

6. ICT Acceptable Use Policy

E-safety is a whole School responsibility, and all Staff and Pupils are required to adhere to an ICT Acceptable Use Policy, which incorporates the following guidelines in age appropriate ways:

6.1 Treating Others with Respect

- The School expects Pupils to treat Staff and each other online with the same standards of consideration and good manners as they would in the course of face-to-face contact. They should always follow the school's Behaviour Policy, which is on the School website.
- The School expects a degree of formality in communications between Staff and Pupils, and would not in normal circumstances expect them to communicate with each other by text or mobile phone.
- Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. The School is strongly committed to promoting equal opportunities for all, regardless of race, gender, religious affiliation, cultural background, gender orientation or disability.

6.2 Cyberbullying

- Cyberbullying is a particularly pernicious form of bullying, because it can be pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. The School's Anti-bullying Policy sets out our preventative measures and the procedures that will be followed where we discover cases of bullying.
- Proper supervision of Pupils plays an important part in creating a safe ICT environment at school; but everyone needs to learn how to stay safe outside of school.
- Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and he or she should not be afraid to report the matter.

6.3 Keeping the School's Network Safe

- Certain sites are blocked by the School's filtering system and the system monitors all use of the network and the IT Manager will oversee the checking of this on a regular basis.
- The system also monitors e-mail traffic and blocks SPAM and certain attachments.
- All Pupils are issued with their own personal school e-mail addresses. Access is via a personal LOGIN, which is password protected. Guidance is given on the reasons for always logging off and for keeping all passwords secure.
- There is strong anti-virus protection on our network, which has been installed by IT Support.
- Any member of staff who wishes to connect a mobile device to the School Staff Wireless Network will be provided with details on how to do this on request.
- Any boarding pupil who wishes to connect a mobile device to the Boarding School Wireless Network will be provided with details on how to do this on request.

Acceptable Use Policies for ICT usage are given to all staff and Pupils. The School will impose sanctions for the misuse, or attempted misuse of the internet, mobile phones and other electronic devices.

7. Technical – Infrastructure/Equipment, Filtering and Monitoring

7.1 The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- There will be regular reviews and audits of the safety and security of School technical systems;
- Servers, wireless systems and cabling are securely located and physical access restricted;
- All users will have clearly defined access rights to School ICT systems. Details of access rights available to groups of users will be recorded by the IT Manager and will be reviewed annually with a member of the School Leadership Team;
- All users will be provided with a username and secure password by the Network Manager who will keep an up to date record of users and their usernames. Users will be required to change their password every 3 months;
- The "administrator" passwords for the School system, used by the IT Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe);
- Users are responsible for the security of their username and password; they must not allow other users to access the system using their log on details and must immediately report any suspicion or evidence that there is a breach of security;
- The School provides enhanced user-level filtering through the use of "Smoothwall". In the event that the IT Manager (or other person) needs to switch off the filtering for any reason, or for any user, it must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader);
- Requests from staff for sites to be removed from the filtered list will be considered by the IT Manager. If the request is agreed, this action will be recorded;
- School IT Support Staff regularly monitor and record the activity of users on the School ICT systems and users are made aware of this in the Acceptable Use Policy;
- Remote management tools are used by staff to control workstations and view user's activity;
- An appropriate system is in place for users to report any actual/potential e-safety incident to the IT Manager (or other relevant person) – see Appendix 2;
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the School systems and data;
- An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the School system;
- The School does not permit specific files to be downloaded on school workstations/portable devices. These files include applications, music files and executable extensions.
- Downloading of copyrighted materials without acquiring appropriate rights for them is not allowed;
- Only IT Support staff are allowed to install programmes on School workstations/portable devices;
- The use of removable media (e.g. memory sticks/CDs/DVDs) by users on School workstations/portable devices is allowed, however they should be scanned for viruses before they are used on the School network;
- The School infrastructure and individual workstations are protected by an up-to-date antivirus software;
- Personal data cannot be sent over the internet or taken off the School site unless safely encrypted or otherwise secured.

8. Curriculum

e-Safety should be a focus in all areas of the curriculum and Staff should reinforce e-safety messages in the use of ICT across the curriculum.

8.1 In lessons where internet use is pre-planned, it is best practice that Pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

8.2 Where Pupils are allowed to freely search the internet, e.g. using search engines, staff will be vigilant in monitoring the content of the websites that the young people visit.

8.3 It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Manager can temporarily remove these sites from the filtered list for the period of study. Any request to do so, should be recorded with clear reasons for the need.

8.4 Pupils will be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of the information.

8.5 Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

9. Bring Your Own Device (BYOD) – Boarding students

9.1 The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by the School of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD. Use of BYOD should not introduce vulnerabilities into existing secure environments and users should refer to the Acceptable Use Policy as well as Parental Information on Mobile Devices, but the following provide a brief overview of the key points:

- The school has a set of clear expectations and responsibilities for all users;
- The school adheres to the Data Protection Act principles;
- All users are provided with and accept the Acceptable Use Policy;
- All network systems are secure and access for users is differentiated;
- Where possible these devices will be covered by the School's normal filtering systems, while being used on the premises;
- All users will use their username and password and keep them safe;
- Pupils receive training and guidance on the use of personal devices;
- Regular audits and monitoring of usage will take place to ensure compliance;
- Any device loss, theft, change of ownership of the device will be reported.

10. Social Networking Sites and Telephone Communication

10.1 The School IT Manager and IT Support staff have a key role in maintaining a safe technical infrastructure at the School and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the School system and data and for training our teaching and support staff in the use of ICT. They monitor the use of the internet and e-mails and will report any observed inappropriate usage to the appropriate senior manager. It is the responsibility of all staff to report any inappropriate usage to the IT Manager. Access to sites of inappropriate content is blocked from the School network, as is access to social networking sites such as Facebook during the school day. (Year 9 and above boarders have access to Facebook in the evenings, but this is monitored by staff in the boarding school on a regular basis).

10.2 In normal circumstances, staff should not share personal contact details with Pupils and this includes mobile telephone numbers, home telephone numbers, instant messaging identities and social network screen-names. Where this is deemed to be needed for any reason, staff should first discuss the matter with the Assistant Head or Preceptor as appropriate. Staff and Pupils should not have each other as contacts on their personal social networking sites. Staff should not request, or respond to, any personal information from the child/young person other than that which might be appropriate as part of their professional role. If queries exist or if advice is needed, staff should consult, in the first instance, the Assistant Head or Preceptor as appropriate.

10.3 Personal e-mail addresses, instant messaging identities or personal telephones (mobile or fixed line) should never be used to contact Pupils without the explicit agreement of the Headteacher, or, in his/her absence, from the Assistant Heads (e.g. school trips).

10.4 The safest approach is to avoid using personal telephone equipment. Staff and Pupils should use school e-mail and can have access to a school mobile telephone for official business.

11. Use of Digital and Video Images – Photographic, Video

11.1 The development of digital imaging technologies has created significant benefits to learning, allowing Staff and Pupils instant use of images that they have recorded themselves or downloaded from the internet. However, Staff, Pupils and parents/guardians need to be aware of the risks associated with publishing digital images on the internet. Those images may provide avenues for cyberbullying to take place; digital images may remain available on the internet indefinitely and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

11.2 The School will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

When using digital images, staff will inform and educate Pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites;

- In accordance with guidance from the Information Commissioner's Office, parents/guardians are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/ guardians comment on any activities involving other Pupils in the digital/video images;
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes;
- Care should be taken when taking digital/video images that Pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute;
- Pupils should not take, use, share, publish or distribute images (for example, video or photographs) of Staff or Pupils without their permission and any images should only be shared with the express permission of those involved;
- Photographs published on the website, or elsewhere that include Pupils will be selected carefully and will comply with good practice guidance on the use of such images;
- A Pupil's work can only be published with the permission of the Pupil and parents or guardians.

11.3 The Terms and Conditions that parents sign includes a section as follows:

*"**Photographs:** You consent to us making use of information relating to your child (including photographs and video recordings) whilst your child is at the School and after he or she has left for the purposes of: (i) managing relationships between the School and current pupils/parents; (ii) promoting the School to prospective pupils/parents; (iii) publicising the School's activities; and (iv) communicating with the school community and the body of former pupils. In respect of (ii), (iii) and (iv), this includes use of such information by the School in/on the School's prospectus (in whatever format or medium), the School's website(s). Parents who do not want their child's photograph or image to appear in any of the School's promotional material must make sure their child knows this and must write immediately to the Head requesting and an acknowledgement of their letter."*

11.4 Staff need to be mindful of the possible child protection issues associated with the possession of images of children and as such they are required to adhere to the following policy.

- All images and video taken of individual pupils or groups of pupils must be uploaded **as soon as possible** to the School network and then **deleted** immediately from any personal computer, the hard drive of any computer, the memory of any camera or similar device, any personal memory device or other transportable memory.
- All images and video of individual pupils or groups of pupils which are delivered to a member of staff as part of their professional work, for example, for an Art display or a marketing initiative, must not be stored on any personal computer, the hard drive of any school computer, the memory of any camera or similar device, any personal memory device or other transportable memory and should be uploaded immediately to the School network.
- Any manipulation or images or video for any purpose including controlled assessment, coursework, marketing, etc., **must** be undertaken on the School network and the results of that manipulation stored on the network only. Exceptionally, Faculty Leaders may have occasion to transmit appropriate video and images to the awarding bodies and will be guided in that by the relevant regulations.

12. Data Protection

12.1 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Kept no longer than is necessary;
- Processed in accordance with the data subject’s rights;
- Secure;
- Only transferred to others with adequate protection.

12.2 Staff must ensure that they:

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

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

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

13. Communications

13.1 A wide range of rapidly developing communication technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighing their risks / disadvantages:

	Staff and other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓				✓			
Use of personal mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓					✓		
Taking photos on mobile phones or other camera devices (only boarders – after school)				✓			✓	
Use of hand held devices e.g. tablets, gaming devices	✓						✓	
Use of personal email address in school, or on school network		✓						✓
Use of school email for personal emails	✓							✓
Use of chat rooms				✓				✓
Use of instant messaging		✓				✓		
Use of social networking sites				✓				✓
Use of blogs	✓						✓	

13.2 When using communication technologies the School considers the following as good practice:

- The official School email service may be regarded as safe and secure and is monitored;
- Users should be aware that email communications are monitored;
- Users must immediately report, to the nominated person, in accordance with the School policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication;
- Any digital communication between Staff and Pupils or parents/guardians (email, chat, etc.) must be professional in tone and content. These communications may only take place on official (monitored) School systems. Personal email addresses, text messaging or social media must not be used for these communications;
- Pupils will be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies and not to include any unsuitable or abusive material;
- Personal information should not be posted on the School website and only official email addresses will be used to identify members of staff.

14. Social Media – Protecting Professional Identity

14.1 All schools have a duty of care to provide a safe learning environment for Pupils and Staff. The School could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the School liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

14.2 The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to Pupils, Staff and the School through limiting access to personal information:

- Clear reporting guidance, including responsibilities, procedures and sanctions;
- Risk assessment, including legal risk.

14.3 School staff should ensure that:

- No reference should be made in social media to Pupils, parents/guardians or School Staff
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the School;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

14.4 The School's use of social media for professional purposes will be checked regularly.

15. Unsuitable/Inappropriate Activities

15.1 The School believes that the activities referred to in the following section would be inappropriate in a School context and that users, as defined below, should not engage in these activities in School or outside School when using School equipment or systems. The School policy restricts usage as follows:

User Actions

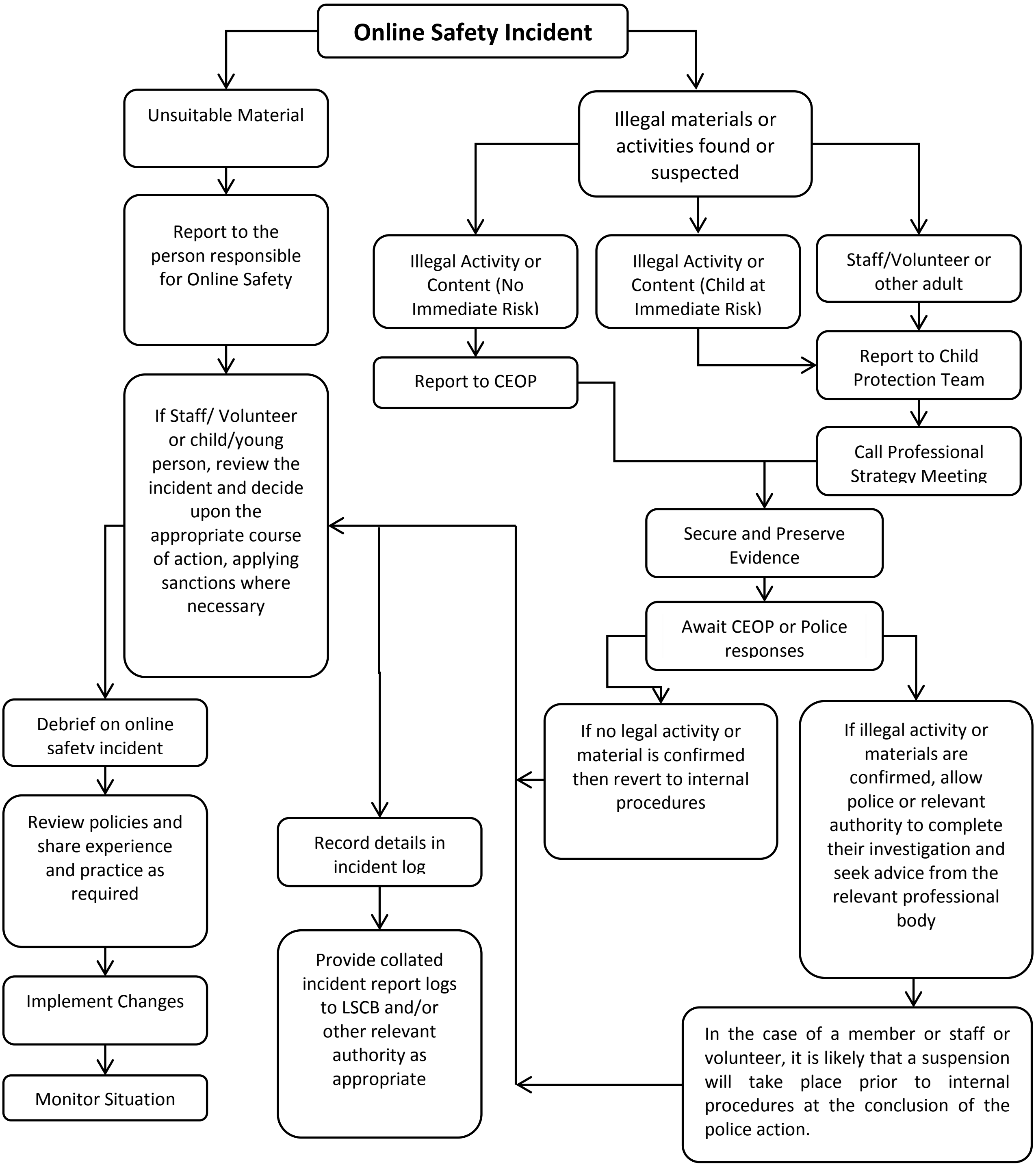
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images -The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					✓
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					✓
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					✓
	criminally racist material in UK - to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					✓	
Infringing copyright					✓	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					✓	
Online gaming (educational)			✓			
Online gaming (non educational)				✓		
Online gambling					✓	
Online shopping / commerce			✓			
File sharing (excludes school collaboration – shared network drives and School Office 365/OneDrive platform)					✓	
Use of social media			✓			
Use of messaging apps			✓			
Use of video broadcasting e.g. Youtube			✓			

16. Responding to Incident of Misuse

16.1 It is hoped that all members of the School community will be responsible users of digital technologies, who understand and follow School policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

16.2 Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



Online Safety Incident
Unsuitable Material
Report to the person responsible for Online Safety
If Staff/ Volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement Changes
Monitor Situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No Immediate Risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection Team
Call Professional Strategy Meeting
Secure and Preserve Evidence
Await CEOP or Police responses
If no legal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member or staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action.

16.3 If any apparent or actual misuse appears to involve illegal activity, the Headteacher will be immediately involved and will report the matter to the Local Authority Designated Officer (LADO) for Child Protection and the police as appropriate (As indicated in the Child Protection Policy).

16.4 Other Incidents

If members of staff suspect that misuse has taken place, but that the misuse is not illegal, it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. More than one member of staff will be involved in the investigation which will be carried out on a "clean" designated computer.

16.5 It is more likely that the School will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Students	Actions/Sanctions								
Incidents:	Refer to class teacher/form tutor	Refer to Faculty Leader/ Senior Teacher	Refer to Assistant Head/e-Safety Coordinator	Refer to Police	Refer to IT Manager for action re filtering/security, etc.	Inform parents/guardians	Warning	Removal of network/internet access rights	Further sanction e.g. detention, exclusion
Deliberately accessing or trying to access material that could be considered illegal			✓	✓		✓		✓	✓
Unauthorised use of non-educational sites during lessons		✓					✓		
Unauthorised use of mobile phone/ digital camera/other handheld device		✓	✓			✓	✓		✓
Unauthorised use of social networking/instant messaging/personal email			✓			✓		✓	✓
Unauthorised downloading or uploading of files		✓			✓			✓	
Allowing others to access the School network by sharing user name and passwords		✓						✓	
Attempting to access or accessing the School network, using another Pupil's account		✓						✓	
Attempting to access or accessing the School network, using the account of a member of staff			✓			✓		✓	✓
Corrupting or destroying the data of other users			✓			✓		✓	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature			✓	✓		✓		✓	✓
Continued infringements of the above, following previous warnings or sanctions			✓	✓		✓		✓	✓
Actions which could bring the School into disrepute or breach the integrity of the ethos of the School			✓	✓		✓		✓	✓
Using proxy sites or other means to subvert the School's filtering system			✓		✓	✓		✓	✓
Accidently accessing offensive or pornographic material and failing to report the incident		✓	✓				✓		
Deliberately accessing or trying to access offensive or pornographic material			✓		✓	✓		✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			✓					✓	

Staff	Actions/Sanctions							
Incidents:	Refer to HOD/Line Manager	Refer to Headteacher	Refer to Human Resources	Refer to Police	Refer to IT Manager for action re filtering/security, etc.	Warning	Suspension	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal		✓	✓					✓
Excessive or inappropriate use of the internet/social networking sites/instant messaging/personal email	✓							
Unauthorised downloading or uploading of files	✓					✓		
Allowing others to access the School network by sharing user name and passwords or attempting to access or accessing the School network, using another person's account	✓							
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓							
Deliberate actions to breach data protection or network security rules		✓	✓					✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓	✓					✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓	✓				✓	✓
Using personal email/social networking sites/instant messaging/text messaging to carry out digital communications with Pupils		✓	✓					✓
Actions which could compromise the staff member's professional standing	✓					✓		
Actions which could bring the School into disrepute or breach the integrity of the ethos of the School		✓				✓		
Using proxy sites or other means to subvert the School's filtering system		✓				✓		
Accidently accessing offensive or pornographic material and failing to report the incident		✓	✓			✓		
Deliberately accessing or trying to access offensive or pornographic material		✓	✓	✓			✓	✓
Breaching copyright or licensing regulations	✓							
Continued infringements of the above, following previous warnings or sanctions		✓	✓					✓

17. Conclusion

ICT has transformed the ways we communicate with others, both in and out of the classroom. Our aim is to promote the positive use of this technology and to discourage inappropriate usage or usage which could put others at risk. Staff are asked to recognise that this policy is designed above all to protect the interests of the child, to support staff and to ensure that required action is taken as quickly as possible.

Appendix 1 – How Will Infringements be handled?

Whenever a Pupil or member of staff infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the School Leadership. The following are set out as guidance based on the level of infringement.

1. Students

Category A Infringements

i. Use of non-educational sites during lessons;
ii. Unauthorised use of e-mail;
iii. Unauthorised use of mobile phone (or other new technologies) in lessons, for example, to send texts to friends;
iv. Use of unauthorised instant messaging/social networking sites.

Possible sanctions: referred to class teacher or tutor for a warning and clarification of what can happen if this is repeated/mobile phone removed from pupil and passed to the Assistant Head for collection at the end of the school day.

Category B Infringements

i. Continued use of non-educational sites during lessons after being warned;
ii. Continued unauthorised use of e-mail after being warned;
iii. Continued unauthorised use of mobile phone (or other new technologies) in lessons after being warned;
iv. Continued use of unauthorised instant messaging/chatrooms/social networking sites;
v. Use of filesharing software for the purposes of sharing music, games or videos illegally;
vi. Accidentally corrupting or destroying others' data without notifying a member of staff about it;
vii. Accidentally accessing offensive material and/or not notifying a member of staff about it;
viii. Not logging off and/or using another students log on details.

Possible sanctions: referred to class teacher or Faculty Leader for follow-up action which could include detention or removal of internet and/or e-mail access for a period of time/mobile phone removed from pupil and passed to the Assistant Head who will contact parents regarding collection of the phone and the length of time when the item cannot be brought into school/referred to the e-Safety Coordinator for a warning of what could happen if this is repeated (particularly for the last two situations)

Category C Infringements

i. Deliberately corrupting or destroying someone's data, violating the privacy of others;
ii. Sending an e-mail or text message that is regarded as harassment or of a bullying nature (one-off);
iii. Deliberately trying to access offensive or pornographic material;
iv. Any purchasing or ordering of items over the internet (without permission from staff);
v. Transmission of commercial or advertising material;
vi. Deliberately using another pupil's login details for malicious purposes and/or passing out your personal login details to another pupil.

Possible sanctions: referred to Assistant Head/Senior Teacher for a warning and clarification of what can happen if this is repeated and contact with parents as well as removal of internet and/or e-mail privileges for a period of time/referred to the e-Safety Coordinator for a warning of what could happen if this is repeated (particularly for the last two situations)/removal of technological device and parent contacted if this is not done via the School network. If inappropriate web material is accessed then ensure the IT Manager is informed and that appropriate technical support filters the site and inform the Assistant Head Pastoral.

Category D Infringements

i. Continued sending of e-mails or text messages regarded as harassment or of a bullying nature after being warned;
ii. Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
iii. Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1998;
iv. Bringing the School name into disrepute;
v. Using the School network as a means of inciting riot or public order offences;
vi. Deliberately trying to circumvent the IT Security Policy.

Possible sanctions: referred to Assistant Head/Headteacher, contact with parents which may include exclusion as well as referral to the Community Police/removal of technological device and parent contacted if this is not done via the School network/ contact with the Child Exploitation and Online Protection Unit.

If appropriate, secure and preserve any evidence, for example, print-outs of e-mails/texts and inform the sender's service provider.

2. Members of Staff

Category A Infringements (Misconduct)

i. Excessive use of Internet for personal activities not related to professional development, for example, online shopping, personal e-mail, instant messaging, etc.;
ii. Use of personal data storage media (for example, USB memory sticks) without considering access and appropriateness of any files stored;
iii. Not implementing appropriate safeguarding procedures;
iv. Any behaviour on the world wide web that compromises the staff members' professional standing in the school and community;
v. Misuse of first level data security, for example, wrongful use of passwords;
vi. Breaching copyright or license, for example, installing unlicensed software on the network.

Possible sanctions: referred to line manager/Headteacher and warning given

Category B Infringements (Gross Misconduct)

i. Serious misuse of, or deliberate damage to, any School computer hardware or software;
ii. Any deliberate attempt to breach data protection or computer security rules;
iii. Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
iv. Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1998;
v. Bringing the school into disrepute.

Possible sanctions: referred to Headteacher/Governors and follow the School's disciplinary procedures; report to Human Resources/involvement of the Police, if appropriate. If there is a safeguarding issue, then remove the PC/laptop to a secure place to ensure that there is no further access to the PC or laptop. If appropriate, instigate an audit of all ICT equipment by an outside agency to ensure there is no risk of pupils accessing inappropriate materials in the School. If appropriate, identify the precise details of the materials. In the case of indecent images of children including child pornography being found, the member of staff will be immediately suspended and the Police should be called. (The School's Child Protection Policy would be implemented.)

Appendix 2 – Reporting e-Safety Concerns

e-Safety Record of Concern

This form should be used to raise e-safety concerns about a pupil or member of staff. It should be used to record non-child protection issues like misuse of the School network or mobile devices. **When completed, this form should be handed to the Senior Teacher or Assistant Head for a pupil and to the e-Safety Coordinator for a member of staff**.

If the matter you are raising is of a child protection nature them please use the paperwork for Welfare Concerns or for Disclosures and pass these details to the Designated Senior Lead or Deputy Designated Senior Lead.

Name of Pupil/ Member of Staff			
Date of Incident			
e-Safety Concern (Please record details of the concern/incident)			
Name (Print)		Date	
Position		Signature	
Report Received by		Date	

Details of Investigation (if relevant)			
Subsequent Actions/ Sanctions			
Name (Print)		Date	
Designation		Signature	

A copy of this document should be passed to the e-Safety Co-ordinator for filing in the Incident Log.