eSafety Policy
Contents

1. Introduction

This policy is one of a series in the college's integrated safeguarding portfolio. Our core safeguarding principles are:

- The college's responsibility to safeguard and promote the welfare of children is of paramount importance.
- Safer children make more successful learners.
- Representatives of the whole-college community (students, parents/carers, staff and governors will be involved in policy development and review.

The policy will be reviewed annually, unless an incident or new legislation or guidance suggests the need for an interim review.

2. Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This eSafety policy will help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement.

However, the use of these new technologies can put young people at risk within and outside the school.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- 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 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.
- Risk of Child Sexual Exploitation (see page 16 Child Protection Policy)

Many of these risks reflect situations in the off-line world and it is essential that this eSafety policy is used in conjunction with other college policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' 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.

This eSafety policy will demonstrate that the College has provided the necessary safeguards to manage and reduce these risks. The policy explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

The school will monitor the impact of the policy using:
- Logs of reported incidents
- Internal monitoring data for network activity

3. Key Personnel

The designated eSafety Coordinator is: Mrs C Singleton / Mrs A Lock

4. Scope of the Policy

This policy applies to all members of the school community (including staff, students, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students/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 eSafety incidents covered by this policy, which may take place out of school and bring the college into disrepute.

The school will deal with such incidents within this policy and associated Behaviour, Child protection and Anti-Bullying policies. (See Appendices A and B)

5. Roles and Responsibilities

The following section outlines the roles and responsibilities for eSafety of individuals and groups within the school.

Governors

- Governors are responsible for the approval of the eSafety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about eSafety incidents and monitoring reports

Head Teacher and Senior Management Team

- The Head Teacher is responsible for ensuring the safety (including eSafety) of members of the college community. The day to day responsibility for eSafety will be delegated to the eSafety Co-ordinator.
- The Head teacher/Senior Management Team are responsible for ensuring that the eSafety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their eSafety roles and to train other colleagues, as relevant
- The Head teacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal eSafety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Management Team will receive regular monitoring reports from the eSafety Co-ordinator.
- The Head Teacher and the Designated eSafety Coordinator should be aware of the procedures to be followed in the event of a serious eSafety allegation being made against a member of staff. (Appendix C and relevant Local Authority HR/disciplinary procedures)

Designated eSafety Coordinator

- takes day to day responsibility for eSafety issues and has a leading role in establishing and reviewing the college eSafety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an eSafety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of eSafety incidents and creates a log of incidents to inform future eSafety developments,
- meets regularly with eSafety Governor to discuss current issues, review incident logs and filtering/change control logs
- reports regularly to Senior Management Team

Network Manager

The Network Manager is responsible for ensuring:

- that the college ICT infrastructure is secure and is not open to misuse or malicious attack
- that the college meets the eSafety technical requirements as advised by Becta and the Acceptable Use Policy.

- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that he/she keeps up to date with eSafety information in order to effectively carry out their eSafety role and to inform and update others as relevant
- that the use of the network/VLE is regularly monitored in order that any misuse/attempted misuse can be reported to the eSafety Co-ordinator for investigation/action/sanction
- that monitoring systems are implemented and updated as agreed in college policies

Teaching and Support Staff
are responsible for ensuring that:
- they have an up-to-date awareness of eSafety matters and of the current college eSafety policy and practices
- they have read, understood and signed the college Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the eSafety Co-ordinator for investigation/action/sanction
- digital communications with students should be on a professional level and only carried out using official school systems. Under no circumstances should staff communicate with students via social networking sites and staff should ensure that privacy settings on personal social networking sites do not allow pupils to access their personal details
- eSafety issues are embedded in all aspects of the curriculum and other college activities
- students understand and follow the college eSafety and Acceptable Use Policy
- students 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 eSafety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current College policies with regard to these devices
- in lessons where internet use is pre-planned students 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

Designated persons for Child Protection
should be trained in eSafety issues and be aware of the potential for serious child protection 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

Students
- are responsible for using the college ICT systems in accordance with the Student Acceptable Use Policy which they will be expected to sign before being given access to college 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 college policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand college policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good eSafety practice when using digital technologies out of school and realise that the college eSafety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, VLE and information about national/local eSafety campaigns/literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student Acceptable Use Policy
- accessing the school website/VLE/online student reports in accordance with the relevant school Acceptable Use Policy.

Community Users

Community Users who access school ICT systems/website/Learning Platform as part of the Extended School provision will be expected to sign/accept a Community User AUP before being provided with access to school systems.

7. Policy Statements

➢ Education and Training

Staff

Training will be offered as follows:

- A planned programme of formal eSafety training will be made available to staff.
- An audit of the eSafety training needs of all staff will be carried out regularly.
- All new staff will receive eSafety training as part of their induction programme, ensuring that they fully understand the school eSafety policy and Acceptable Use Policies
- The eSafety Coordinator will receive regular updates through attendance at LA/other information/training sessions and by reviewing guidance documents released by BECTA and others.
- This eSafety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The eSafety Coordinator will provide advice/guidance/training as required to individuals as required

Students
Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in eSafety is therefore an essential part of the college eSafety provision. Children and young people need the help and support of the school to recognise and avoid eSafety risks and build their resilience. eSafety education will be provided in the following ways:

- A planned eSafety programme is provided as part of ICT/PHSE lessons – this will cover both the use of ICT and new technologies in school and outside school
- Key eSafety messages will be reinforced as part of a planned programme of assemblies and classroom activities
- Students 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
- Students will be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems/internet will be posted in all rooms
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Parents/Carers
Many parents and carers have only a limited understanding of eSafety 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 experiences. Parents often either underestimate or do not realise 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 digital divide". (Byron Report).

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

- Letters, newsletters, web site, VLE
- Parents evenings/Review days

Governors
Governors should take part in eSafety training/awareness sessions, with particular importance for those who are members of any committee/group involved in ICT/eSafety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or other relevant organisation.
- Participation in college training/information sessions for staff or parents

➢ Technical

Infrastructure/equipment, filtering and monitoring

The college is responsible for ensuring that the school 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 eSafety responsibilities:

- College ICT systems will be managed in ways that ensure that the school meets the eSafety technical requirements outlined by Becta and the Acceptable Usage Policy
- College ICT systems will be regularly updated to ensure up-to-date anti-virus definitions and Microsoft Windows Security Updates are installed. Essential software i.e. Acrobat Reader, Flash Player, Java, Internet Explorer, Smartboard etc. must be kept current.
- There will be regular reviews and audits of the safety and security of college ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the eSafety Committee.
- All users will be provided with a username and password to access the school network 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 at least annually.
- All users of the College VLE will be provided with a username and password for secure access in school and beyond.
- The "administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Head Teacher or other nominated senior leader and kept in a secure place (eg school safe)
- A school should never allow one user to have sole administrator access
- College Data should be securely managed when taken off the school site using encrypted memory devices or password protected files.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- In the event of the Network Manager needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head Teacher.

➢ Curriculum

- eSafety should be a focus in all areas of the curriculum and staff should reinforce eSafety messages in the use of ICT across the curriculum.
- eSafety should be taught regularly through a scheme of work with identified progression of knowledge, skills and understanding.

- eSafety skills should be embedded through both discrete ICT and cross-curricular application.
- In lessons where internet use is pre-planned, students 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.
- Where students are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites visited.
- Students should 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
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

➢ **Use of digital and video images - Photographic, Video**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The college 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 should inform and educate students 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 eg on social networking sites.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of students are published on the school website
- Students' work can only be published with the permission of the student/pupil and parents or carers.

➢ Data Protection

Staff should 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.
- Are aware that email communications may be monitored
- Do not post personal information on the school website
- Only use official centrally located email addresses (ie schooloffice@stjohnplessington.com) to communicate with parents/pupils.

➢ Unsuitable/inappropriate activities

The college believes that the activities referred to below would be inappropriate in a school context and that staff and students should not engage in these activities in school or outside school when using school equipment or systems.

Users must 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
- promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in UK
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- 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 college or brings the college into disrepute

The following are also unacceptable when using college equipment or systems:

- Using college systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Creating or propagating computer viruses or other harmful files
- Revealing or publicising confidential or proprietary information (eg financial/personal information, databases, computer/network access codes and passwords)
- Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet
- Online gambling

- **Responding to incidents of misuse**

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

If any apparent or actual misuse appears to involve illegal activity:

Appendix D should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence should be adhered to. Guidance should also be taken from the college Child Protection Safeguarding Policy.