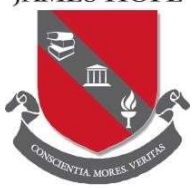
JAMES HOPE



COLLEGE

JAMES HOPE COLLEGE – ESAFETY POLICY

Policy Statement

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

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

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

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

Wider College community – students, all staff, governing body, parents.

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

The primary purpose of this policy is two-fold:

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

This policy is available for anybody to read on the James Hope College's SharePoint. Upon review all members of staff will sign as read and understood both the 'e-safety policy' and the 'Staff Acceptable Use' Policy. A copy of this policy and the Students Acceptable Use Policy will be sent home with students at the beginning of each College year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to College technology including the Internet.

Policy Governance - Roles & Responsibilities

Governing Body

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

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up-to-date, covers all aspects of technology use within the College, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of e-safety at the College who will:
  - Keep up-to-date with emerging risks and threats through technology use.
  - Receive regular updates from the Principal in regards to training, identified risks and any incidents.
  - Chair the e-Safety Committee

The Principal

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

The Principal will ensure that:

- E-Safety training throughout the College is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team (SLT) and governing body, parents.
- The designated e-Safety Coordinator has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

E-Safety Coordinator

The day-to-day duty of e-Safety Coordinator is devolved to VP ICT/InnovationsThe

e-Safety Coordinator will:

- Keep up to date with the latest risks to children whilst using technology; familiarize himself with the latest research and available resources for College and home use.
- Review this policy regularly and bring any matters to the attention of the Principal.
- Advise the Principal, governing body on all e-safety matters.
- Engage with parents and the College community on e-safety matters at College and/or at home.
- Liaise with the local, state and federal arms of government, IT technical support and other agencies as required.

- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in College (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the Cyberspace and/or ICT Technical Support.
- Make himself aware of any reporting function with technical e-safety measures, i.e., internet filtering reporting function; liaise with the Principal and responsible governor to decide on what reports may be appropriate for viewing.

IT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any e-safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that category of use are discussed and agreed with the e-safety Coordinator and Principal.
    - Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters.
    - The IT System Administrator password is to be changed on a monthly (30 day) basis.

All Staff

Staff are to ensure that:

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

All Students

The boundaries of use of ICT equipment and services in this College are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

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

Parents and Carers

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

Parents must also understand the College needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to College ICT equipment or services.

E-Safety Committee

Chaired by the Governor responsible for e-Safety, the e-safety Committee is responsible to:

- advise on changes to the e-safety policy.
- establish the effectiveness (or not) of e-safety training and awareness in the College.
- recommend further initiatives for e-safety training and awareness at the College.

Established from volunteer students, parents, e-Safety Coordinator, responsible Governor and others as required, the e-Safety Committee will meet on a termly basis.

Technology

James Hope College uses a range of devices including PC's, laptops, Apple Macs. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

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

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

Encryption – All College devices that hold personal data are encrypted. No data is to leave the College on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e., loss/theft of device such as laptop or USB pen drives) is to be brought to the attention of the Principal

immediately. The Principal will liaise with the governing body to ascertain whether a report needs to be made to the Chairman. *(Note: Encryption does not mean password protected.)*

Passwords – all staff and students will be unable to access any device without a unique username and password. Staff and student passwords will change on a termly basis or if there has been a compromise, whichever is sooner. The e-safety Coordinator and IT Support will be responsible for ensuring that passwords are changed.

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

Safe Use

Internet – Use of the Internet in College is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.

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

Students are permitted to use the College email system, and as such will be given their own email address.

Photos and videos – Digital media such as photos and videos are covered in the Colleges' Photographic Policy and is re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

Social Networking – there are many social networking services available; James Hope College is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider College community. The following social media services are permitted for use within James Hope College and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the e-Safety Coordinator who will advise the Principal for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in College.
- Twitter – used by the College as a broadcast service (see below).
- Facebook – used by the school as a broadcast service (see below.

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

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

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

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

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

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

E-Safety for students is embedded into the curriculum; whenever ICT is used in the College, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

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

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

E-Safety Training Programmes will be announced regularly.