THE LADIES COLLEGE, MELROSE and
THE LADIES COLLEGE PRE-PREPARATORY DEPARTMENT

ACCEPTABLE USER POLICY (E-NET SAFETY)

1. Introduction

The purpose of this policy document is to define the principles and aims of communication at Melrose and to provide a framework which;

- promotes consistency in school planning and school practice.
- facilitates development and change.
- informs new staff, pupils, parents, governors and the wider community.

This policy was reviewed in Michaelmas Term 2015. The next review will be in the Michaelmas Term 2016.

This policy should be viewed in conjunction with the Melrose ICT policy, the Senior School ICT policy and all subject policies where ICT is a resource, in addition to the Child and Data Protection policies, Anti-Bullying policy and Behaviour and Discipline policy.

2. Roles and responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the Ladies' College, Melrose and the Ladies' College Pre-Preparatory Department.

- The Head Teacher in conjunction with the Ladies' College senior school Head of Department for ICT is responsible for ensuring the e-safety of members of the Melrose and Ladies' College Pre-Preparatory Department community.
- The designated e-safety coordinator for the Ladies' College is the Head of Department for ICT at Ladies' College senior school.
- Members of the Melrose Senior Leadership Team when responding to incidents of misuse will report the incident to the e-safety coordinator.
- The e-safety coordinator receives regular CPD in e-safety procedures and is responsible for providing training, support and advice to other colleagues as necessary.
- The e-safety safety coordinator liaises with school ICT technical staff.
- The e-safety coordinator receives reports of e-safety incidents and records them in an agreed reporting format to inform future e- safety developments for the College.
- The e-safety coordinator reports to the Deputy Principal who will in turn inform the College SMT of any concerns.
- The e-safety coordinator receives training in the child protection issues associated with sharing of personal data, access to illegal/inappropriate materials, inappropriate online contact with adults/strangers, potential or actual incidence of grooming and the avoidance of cyber bullying.

Teaching and support staff are responsible for:

- ensuring that they have read and understood the Ladies ' College Melrose and Ladies' College Pre-Preparatory Department e-safety policy.
- reporting any suspected incidents of misuse to The Head Teacher and e-safety coordinator.
- ensuring that any digital communications with pupils e.g. email or virtual learning environment are carried out on a professional level using only the College systems.

- guiding pupils to ensure that they know how to use the Internet safely and how to deal with any unsuitable material that is found.

3. Aims

We aim to:

- equip children, their parents or carers and staff to stay safe online by keeping them informed of e-safety procedures adopted by the school and promoting e-safety messages in home use of ICT.
- be data protection compliant by using personal data only on secure password protected computers and ensuring that correct 'logging off' takes place at the end of any session involving personal data.
- ensure that pupils, parent, carers and staff are responsible users and stay safe whilst using the Internet or other communications technologies for educational, personal or recreational use.
- protect the school ICT systems and users from accidental or deliberate misuse that could put the security of the systems and users at risk, through the Guernsey Grid for Learning and The Ladies' College systems, such responsibility being held by the Head of ICT
- to foster individual responsibility for actions both in and out of school
- restrict access by ensuring a member of staff is always present when computers are being used and requiring that any pupil that brings a mobile phone to school gives it to the school secretary for safe keeping during the day.

4. Curriculum

E-Safety is a focus of all areas of the curriculum.

- Where use of the Internet is pre-planned, pupils will be guided to sites checked as suitable for their use. Where pupils are allowed to freely search the Internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the girls will visit. All access to the Internet is filtered through the Guernsey Grid for learning but staff should remain vigilant in case unsuitable material remains unfiltered.
- During their time at Melrose the girls will be taught to be critically aware of the materials/content that they access online and they will be guided to validate the accuracy of the information.
- E-safety messages may be reinforced in PSHE, Assemblies and all lessons involving use of ICT.
- ICT will be used to enhance and extend education beyond the classroom.
- ICT will be used to help pupils to become independent learners.
- Pupils will be taught to select appropriate software tools at the point of need.

Use of digital and video images

- Staff are allowed to take digital/video images to support educational aims but must ensure that they use school equipment (cameras, camcorders etc) to do so.
- Care should be taken when taking digital/video images that girls are appropriately dressed and are not participating in activities that might bring the individual or College into disrepute.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance, including the States Education Department (SED) guidance on the use of photographic images of children, on the use of such images.
- Written permission for the use of photographic images for publications such as the school magazine, prospectus and handbooks will be sought from parents or carers, when a pupil joins the College.
- Melrose pupils who bring mobile phones or other handheld devices to school leave them with

the school secretary for safe keeping during the day. Pupils may use school hand held devises but are not permitted to publish images taken using those devises outside school.

Data protection

Personal data will be recorded, processed, transferred and made available according to the data protection (Bailiwick of Guernsey) law 2001.
Staff must ensure that they:

- take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on a secure password protected computer or other device, ensuring that they are properly "logged off" at the end of any session in which they are using personal data.

5. Resources

- Head of ICT and ICT technicians, based at the Senior School but responsible for the Junior School.
- PSHE lessons, Assemblies and all lessons involving use of ICT.
- Notices strategically placed around the school, telling children where to go for help if they are worried or have any concerns.
- Guernsey Grid for Learning
- www.thinkuknow.co.uk CEOP – Child Exploitation and Online Protection is the UK centre of excellence for helping safeguard children from online threats and has very good links to PSHE and citizenship
- www.childnet.com offers good advice for cyberbullying
- www.cybermentors.org.uk good site where children can ask questions
- www.netsmart.org for KS1 and KS2
- CEOP The Child Exploitation and Online Protection Centre. www.ceop.police.uk
- Appendix 1

6. Reporting

Discretion will be used at all times
Staff discussion and verbal feedback to staff involved
The Headteacher and Principal should be made aware of all allegations and incidents.
Parents may be informed if or when appropriate.

Appendix 1

New technologies have become integral to the lives of children and young people in today's society, both within schools and their lives outside school. The Internet and other digital information and communication technology are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe Internet access at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the Internet and other communication technology for educational, personal and recreational use. That College ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk. That staff are protected from potential risk in their use of ICT in their everyday work.
- The College will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils and will in return expect staff and volunteers to agree to be responsible users.

For my professional and personal safety:

- I understand that the College will monitor my use of ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to the use of school ICT systems (e.g. laptops, email,) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the College.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal or inappropriate or harmful material or incident, I become aware of, to the Head of Department for ICT (e – safety coordinator.)
- I will be professional in my communications and actions when using the College ICT systems
- I will only use chat and social networking site in College in accordance with the College policies.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use policy agreement, I could be subject to disciplinary action. This could include a warning or a suspension, and in the event of illegal activities the involvement of the police.

Signed: