

Appendix C – Example of User SyOps

Scope

The following Security Operating Procedures (SyOps) apply to all *(insert system name)* users, independent of any explicit role they may have on the system. All *(insert system name)* users have to comply with these SyOps, in addition to those specific to their roles.

Remember, non-compliance with the SyOps may lead to disciplinary action being taken against you.

General “Dos and Don’ts” for all *(insert system name)* staff

As a *(insert system name)* User, you are to:

- Sign as having read and understood the Security Policy and SyOps produced for *(Insert system name)* and the security obligations stated in it. The *(insert system name)* Head Teacher will ask you to do so before commencement of work on *(insert system name)*;
- Attend and implement any security briefings provided by the Head Teacher for all staff working on *(insert system name)*;
- Consult the Head Teacher regarding any proposed changes to *(insert system name)*. These changes could be changes to software, hardware, design, the technical architecture or any procedural changes;
- Ensure that all changes to *(insert system name)* are clearly documented and that adequate reports and logs are maintained and that they are accountable to you;
- Comply with the *(insert system name)* Incident Management Procedures. You are to promptly report any unusual suspected or detected attempts to breach security to the Head Teacher or Network Manager. You can contact the Network Manager by phone:, pager: or email: The Network Manager is to inform the Head Teacher at the earliest opportunity;
- Report all security incidents involving a breach of personnel, hardware, software, communication, document or physical security immediately to the Network Manager and Head Teacher. Keep written details of these incidents for any investigation to follow;
- Complete a “Security Incident Report Form” *(insert where this can be found)* and forward it to the Network Manager as soon as practicable. Examples of security breaches are:
 - unauthorised or unescorted visitors;
 - unauthorised access to the institution;
 - compromise of passwords;
 - unauthorised introduction of software;
 - unauthorised modification or tampering with components;
 - unattended terminals left logged in; and,
 - theft of hardware or software.
- Ensure that evidence is collected by the Network Manager and not tampered with in the event of a security incident. You are to co-operate with the Network Manager during such investigations;
- Comply with the *(insert system name)* Clear Desk and Clear Screen Policy:
 - Lock away all sensitive and valuable documents (paper and magnetic) in cabinets or desk drawers (as appropriate) when the desk is unattended for an extended period - for example when away for meetings, at lunch times, or overnight;
 - Log off computers and laptops (unless a password protected screen saver is in operation on the workstation) when unattended. When you have finished a session on the workstation invoke the password-protected screensaver and at cease of work close down all the applications and log off/shutdown the workstation/laptop and lock the laptop away or secure it through the use of a cable lock;
 - If, in an emergency, you need to leave the office quickly, such as a fire alarm, invoke the password-protected screensaver, ONLY IF IT IS SAFE TO DO SO, so that unauthorised personnel cannot use it; and,
- Obtain authorised permission from the Head Teacher/Network Manager when removing any equipment from Institution premises. Each piece of equipment is to be signed out and

returned on time. The Network Manager will check this at set intervals to confirm that they have been returned on time;

- Follow the procedures developed by the *(insert system name)* Head Teacher to protect unattended User equipment from loss, damage or theft both on-site and off-site;
- Comply with *(insert system name)* ICT security and Back-Up Procedures: virus check the contents of all email messages used in conjunction with *Insert system name* and notify the Network Manager if you suspect any malicious code, such as viruses and trojan horses;
- Ensure that any documents or magnetic media, or other removable media such as CDs, DVDs and so on, you use are given the correct sensitivity labelling, and if necessary are registered and secured in an appropriate security container;
- Remember that it is a fundamental principle that knowledge or possession of sensitive information is to be strictly limited to those Users that have a need to know and appropriate privileges. *(insert system name)* Users are to adhere to this principle;
- Comply with the *(insert system name)* Acceptable Use Policy:
 - If you need an account on a *(insert system name)* server you will need the approval of the *(insert system name)* Head Teacher, or in their absence, the Network Manager. Once approved the Head Teacher will instruct the *(insert system name)* Network Manager to have your account created; and,
 - You will need to notify the *(insert system name)* Head Teacher if your access requirements change.
- Challenge anyone you do not recognise, if you are suspicious of that person report to the Institution office by the quickest means;
- Ensure that laptops are secured with cable locks when left unattended;
- Make sure that anti-virus software, and personal firewall software is installed, up to date, and active on laptops that you use for access to *(insert system name)*. For advice on correct configuration of laptops, contact the Network Manager;
- Comply with the *(insert system name)* Password Policy

As a *(Insert system name)* User, you are NOT to:

- Make any changes to *(insert system name)* without following the policies for change control;
- Load software (such as computer games) onto *(insert system name)* equipment without prior consent of the network manager. or use it concurrently on workstations, while *Insert system name* sessions are open;
- Disable the anti-virus software resident on workstations or laptops;
- Test *(insert system name)* security features or use any software or tools to examine the network or workstations without authority.
- Attempt to gain unauthorised access to *(insert system name)*;
- Attempt to use *(insert system name)* under another identity (UserID) or share your password with anyone else;
- Attempt to access information outside of your normal access rights or duties. You will be responsible for all actions undertaken on *(insert system name)* using your UserID;
- Disclose your password. You are to contact your administrator to change your password if your password has become disclosed or you are instructed to by the system.