

Highgate School

IT Acceptable Use Policy

Information Technology Guidelines for Staff and Pupils

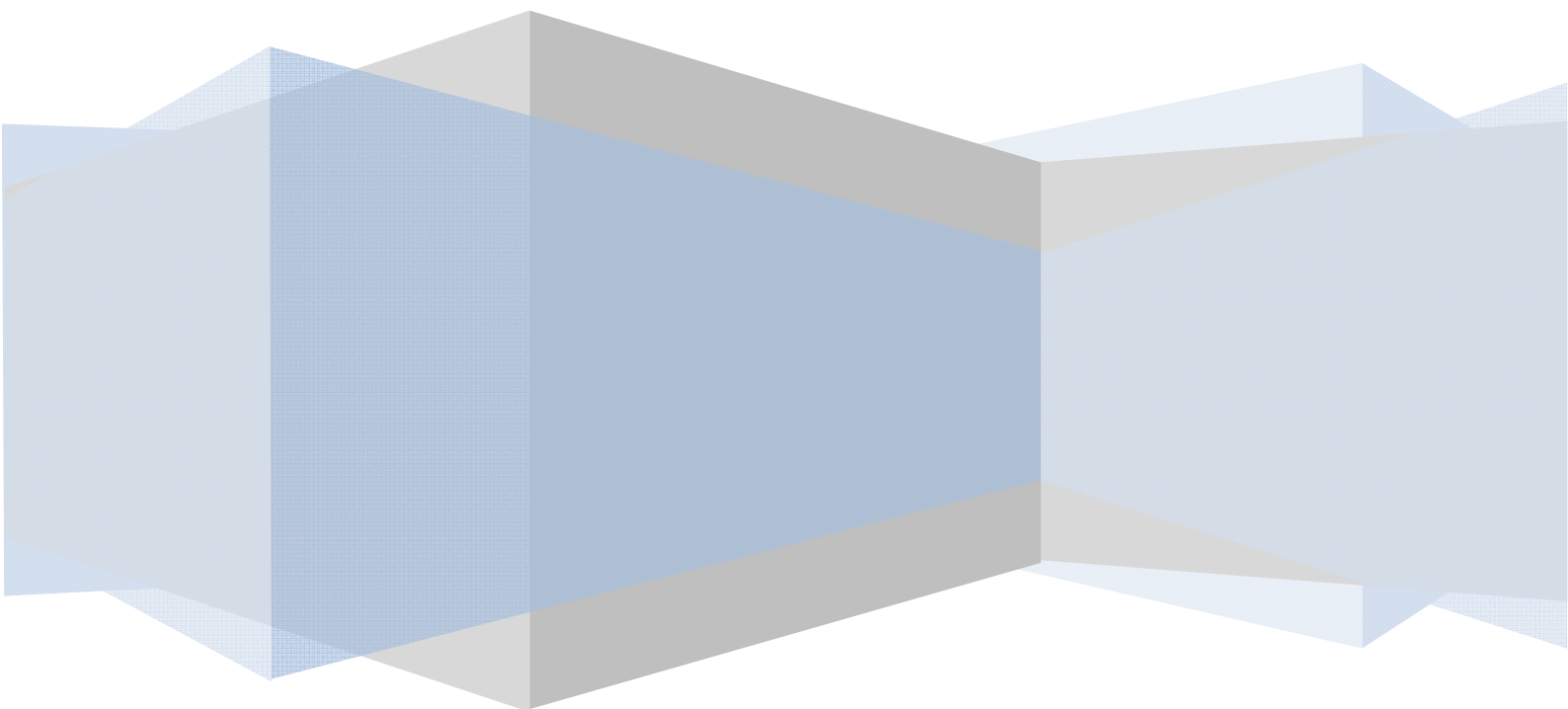
Author: IT Department

Date: 05/09/2008

Version: 1.1

Updated: September 2009

To be reviewed by working party in October 2009



Contents

1. Scope	3
2. Definitions	3
3. Relevant Legislation.....	3
4. Use of Facilities and Learning Resources	4
5. Monitoring of IT Facilities.....	6
6. Maintenance & Repairs	7
7. Copyright and Licence Agreements.....	8
8. Behaviour	8
9. Infringement.....	8
10. Disclaimer	9
Appendix 1 – Facebook.....	10
Appendix 2 – Email Good Practice	11
Appendix 3 – Technology Policy Overview for Pupils	13

Highgate School IT facilities must be used correctly and not misused or abused by users. This includes electronic services such as Email and Internet access. All staff and pupils should be committed to conforming to good practice in this area. Use of the School's IT facilities implies acceptance of the conditions of use. This document sets out current policy and practice; this document is reviewed regularly and can change without notification.

1. Scope

The following regulations apply to users of all IT facilities and learning resources owned, leased or hired by the School, all users of such facilities and resources on the School's premises and all users of such facilities and resources connected to the School's networks.

Staff and pupils should note the consequences of failing to comply with these regulations as set out in section 9 (Infringement), particularly that disciplinary action may be taken by the School for failure by a user to comply with them and that they may be charged for the School's costs arising out of such failure. The School is defined as Highgate School and refers to the entire Foundation.

2. Definitions

Portable Computers - Laptop and Notebook computers owned, leased or hired by the School.

Desktop Computers – Static Desktop & Workstation computers owned, leased or hired by the School.

Users - All staff and pupils of the School and others outside the Foundation who have been given permission to use the School's IT facilities and learning resources.

Facilities - IT facilities located in the School, including networks, servers, desktop computers and portable computers, together with the software and data stored on them. Any IT use carried out on equipment connected to the School network, whether or not this involves the use of an School-based or School-owned computer.

Learning Resources - All learning resources including (but not exclusively) text, video, audio which are available to the School's users.

Designated Authority - The Designated Authority refers to the School's IT Services Manager and Senior Management Team (SMT). The Designated Authority may delegate responsibility for particular areas to appropriate School staff.

3. Relevant Legislation

Users must comply with all UK legislation relating to the use of information, computers and networks. Applicable laws include, but are not limited to:

a. **Data Protection Act 1998.** This act makes provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

b. **Copyright, Designs & Patents Act 1988.** Copyright material includes literary works (including computer software), artistic works (including photographs), sound recordings (including music), films (including video) and databases.

c. **Computer Misuse Act 1990.** The act provides safeguards for computer material against unauthorised access or modification.

d. Privacy and Electronic Communications (EC Directive) Regulations 2003.

These regulations prohibit the sending of unsolicited marketing emails (or SMS/text messages) to individuals. In addition, the regulations control the use of 'cookies'¹.

e. Fraud Act 2006. The Act prohibits 'phishing' whereby official-looking emails guide unsuspecting users to fake websites (e.g. fake bank websites) in order to steal their login details. Creating or possessing software to enable this activity is also an offence.

4. Use of Facilities and Learning Resources

Personal Use

The School's IT facilities are provided for educational, administrative, research and personal development use by staff in the course of their employment and by pupils in the course of their education. Any other use of the School's resources puts an additional demand on those resources, which affects their performance.

Limited personal use of certain facilities is permitted, during personal time. Any such use must neither interfere with the employee's own work or the student's study, nor prevent others from pursuing their legitimate work and use of the School's IT facilities. The school reserves the right to withdraw this benefit either individually or collectively at any time. In such circumstance the School will endeavour to give reasonable notice of its intention to withdraw such benefit.

Where the School becomes aware of a specific type of personal use which affects the efficient operation of its IT facilities, the School will take appropriate steps to withdraw, without notice, access to the relevant facility or resource. Non-exhaustive examples of this include barring access to certain technology or Internet resources such as web sites, news groups or other Internet resources. Users who have a legitimate requirement to access such withdrawn resources should discuss the matter with the Designated Authority. The fact that a user is able to access a particular technology or resource does not necessarily imply that the technology or resource may be accessed in accordance with these Regulations.

Commercial Use

Use of any of the School's IT facilities for commercial gain (including advertising) or for work on behalf of others (unconnected with a student's course of study at the School or a member of staff's legitimate activities) is prohibited, unless the User has explicit prior written permission of the Designated Authority and an appropriate charge for such use has been contractually agreed between the other party and the School.

Movement

School IT facilities, with the exception of portable computers should not be moved or disconnected without the prior agreement of the Designated Authority.

Connection - Network Access

¹ This is a collection of information, usually including a username and the current date and time, stored on the local computer of a person using the Internet. It is used by websites to identify users who have previously registered or visited the site.

Users must not connect any personal device into the School's network or other IT facility without prior agreement from the Designated Authority.

Damage

Users must not cause any form of damage to the School's IT facilities, software, or to any of the rooms and their facilities and services which contain that equipment or software. The term 'damage' includes any unauthorised installation of hardware or software, which incurs time and/or cost in restoring the facilities to their original state.

Security

Users must not deliberately introduce any virus, worm, Trojan horse or other harmful or nuisance program or file into any IT facility, nor take deliberate action to circumvent any precautions taken or prescribed by the School to prevent this. Users must not attempt to penetrate the security and/or privacy of other users' files. All of the School's IT facilities have anti-virus and anti-spyware protection installed.

Spam and Mass-circulation

Spam is usually defined as unsolicited electronic messages (using email, SMS, Instant Messaging or other means) sent in bulk. Users may not use School IT facilities to send Spam.

Sending unsolicited electronic messages for the purposes of marketing is prohibited under the Privacy and Electronic Communications (EC Directive) Regulations 2003.

Illegal and/or Offensive Material

Users must not use School IT facilities to access, produce, obtain, download, store, view, share, or distribute material (including images, video, text or sound files) which is either illegal under UK law (e.g. in breach of copyright law) and/ or can reasonably be judged to be offensive, likely to incite racial hatred, obscene, indecent, or abusive. The only exceptions would be where such material, which may be judged offensive, is essential for research or teaching, is permitted by law, and prior permission has been granted by the Designated Authority.

Discrimination

Users must not use the School's IT facilities to place, disseminate or receive materials which discriminate or encourage discrimination on, for example, the grounds of gender, sexual orientation, disability, age, religious belief, race or ethnic origin.

Defamation

Users must not use the School's IT facilities to publish any information which

- they know or believe to be untrue
- is defamatory and could not be defended on the grounds that it is true/factual or that it is fair comment on a matter of public interest (e.g. works of literature, art, music, television and radio or the activities of public figures)

5. Monitoring of IT Facilities

In order to protect the security and working of the School's IT facilities & users, it may be necessary to monitor collective or individual usage of its IT facilities. This is particularly likely where there are indications of abuse of systems, or that individuals may be using systems in excess of their authority. Files, messages, emails and user account information may be intercepted, monitored, recorded, copied, audited, and inspected.

Confidentiality

Absolute confidentiality cannot be guaranteed. Any emails or files, stored and/or sent or received may be accessed by colleagues other than the individual to whom it was intended for, whether by accident (e.g. a computer left logged on) or design (e.g. an email may need to be opened to diagnose connectivity problems which have been brought to the attention of the IT department.). Emails and files cannot therefore be regarded as totally private or confidential. Personal email messages and files should be written remembering this possibility for third parties to review the content. In the case of external (Internet) Email, there cannot be an absolute guarantee of security. Such emails can potentially be intercepted and read by third parties without our knowledge. Messages of particular confidentiality or sensitivity should be sent by an alternative medium.

The IT department have total administrative access to all of the School's IT facilities. The IT department have the right to monitor and access all IT resource, this includes any saved files. Any misuse of IT facilities found by the IT department will be reported to the Designated Authority.

Internet Access

Internet access is provided for educational, administrative, research and personal development use. It should be noted that users of the Internet do not have a right to confidentiality or privacy when using or accessing the School's IT facilities. The Designated Authority monitors and reviews network logs maintained in order to ensure compliance with School policies and UK law. The School uses monitoring software to track usage. This software records details of every web site visited, along with the relevant user name and date/time, and produces regular reports for monitoring purposes. Misuse, or visits to sites of an improper nature, will automatically be reported to the Designated Authority.

Email

The School reserves the right to retrieve the contents of messages for the following purposes:

- to monitor whether the use of the e-mail system is legitimate and in accordance with this policy;
- to find lost messages or to retrieve messages lost due to computer failure;
- to assist in the investigation of wrongful acts;
- to comply with any legal obligation.

Monitoring will only be carried out to the extent permitted or required by law. The School will not routinely monitor e-mail messages. Spot checks or tailored searches may be undertaken in the context of disciplinary proceedings (whether actual or contemplated) or

where the School has reason to believe that the systems may be being used in breach of this policy.

The School's policy towards spam is that it should be filtered upon receipt and quarantined. All effort is made to filter out spam before reaching users' inboxes, however it should be kept in mind that spam filtering is an ongoing endeavour and therefore not fool-proof. The occasional message may reach a user and should be deleted in the normal way. Measures are taken to ensure that no false-positives (legitimate messages treated as spam) are filtered, however it is possible that the occasional message is falsely identified as spam. In such cases the quarantine email can be released by the IT department.

Files

The School reserves the right to retrieve the contents of files for the following purposes:

- to monitor whether the use of the storage medium is legitimate and in accordance with this policy;
- to find deleted files or to retrieve files lost due to IT facility failure;
- to assist in the investigation of wrongful acts;
- to comply with any legal obligation.

Monitoring will only be carried out to the extent permitted or required by law. The School will not routinely monitor files. Spot checks or tailored searches may be undertaken in the context of disciplinary proceedings (whether actual or contemplated) or where the School has reason to believe that the systems may be being used in breach of this policy.

Storage – Personal Folder (Z Drive) and Departmental Shares

Each user receives a personal folder, which is private to them and accessible via the network. A maximum quota is imposed to prevent the server from being filled by a few users. This folder is allocated the drive letter (Z:). It is often referred to as "Your Z drive".

Please note that the IT department have administrative privileges and access to your personal folder and all files stored on the School's IT facilities. Please do not store personal photos or music files in personal folders; it is designed for storing work documents only.

Software

Users of the School's network are not authorised and are unable to load any software onto the IT facilities. Only software licensed to the School may be installed on the School's IT facilities. It is forbidden, under any circumstances, to run peer to peer (P2P) software such as Kazaa, eDonkey, BitTorrent or Limewire on any of the School's IT facilities.

Software downloaded from the Internet and/or software obtained illegally must not be loaded onto the School's IT facilities. Any software obtained and/or installed illegally will be reported to the Designated Authority.

6. Maintenance & Repairs

Maintenance is to be controlled by the IT Department in conjunction with external suppliers. From time to time IT facilities especially portable computers will be recalled by IT

Support for maintenance purposes. It will not be possible to properly support the School's IT Facilities if equipment is not correctly maintained. Any faulty/out of order IT facility should be reported to the IT department as soon as the problem is found. Any data stored on faulty IT facilities will be recovered using a "best effort" approach by the IT department. Any cost incurred by the IT department in recovering data may be charged back to the user or department involved.

If any IT facilities require external repair, The IT department will take a "best effort" approach to remove all data ahead of repair.

7. Copyright and Licence Agreements

Users must adhere to the terms and conditions of all licence agreements relating to IT facilities and learning resources, which they use including software, services documentation and other goods.

Users must not copy or modify any copyright material (3rd party material) nor incorporate any part of the 3rd party material into their own work unless such acts are either permitted under the CDP Act 1988, by a Licence Agreement, or with the permission of the copyright holder.

Users must not install, make, store, or transfer unlicensed copies of any copyright or trademark work including software, videos or music, unless permitted under legislation or with the permission of the copyright holder.

8. Behaviour

Users must respect the rights of others and should conduct themselves accordingly when using IT facilities to create a beneficial environment for all.

Users must not interfere with or disrupt the availability and use of the IT facilities by others. Users must take every precaution to avoid damage to equipment and learning resources caused by the presence of food and drink in its vicinity. Under no circumstances must food or drink be consumed near any IT facilities.

9. Infringement

Withdrawal of facilities - If a User is in breach of any of these regulations, the Designated Authority may withdraw or restrict the User's use of IT facilities and learning resources, following consultation with the User's head of department or in relation to pupils their form tutor, head of year/house and/or parents.

Removal of Material - The School reserves the right to remove material from its IT facilities without notice where such material is in breach of these regulations.

Disciplinary action - Any breach of the regulations may be dealt with by the Designated Authority under the School's formal disciplinary procedure for both pupils and staff and in some cases may result in suspension, expulsion or dismissal. The User may be charged for any costs that have arisen as the result of misuse or abuse of facilities and/or resources.

Breaches of the law - Where appropriate, suspected breaches of the law may be reported to the police. Where the breach has occurred in a jurisdiction outside the UK, the breach may be reported to the relevant authorities within that jurisdiction.

10. Disclaimer

The School accepts no responsibility and expressly excludes liability to the fullest extent permissible by law, for:

- the malfunctioning of any IT facility or part thereof, whether hardware, software or other,
- the loss of any data or software or the failure of any security or privacy mechanism.

Staff Guidelines for the use of Facebook.com

General Practice and Advice

- Members of staff should not be in contact with current Highgate pupils via social networking sites such as Facebook.com, in accordance with the School's Safeguarding and Welfare policy.
- Members of staff with Facebook profiles should set the privacy levels on their accounts to maximum i.e. only people on their friend's list should be able to view their pictures/private information etc. This can be done by going to **Setting > Profile** and adjusting the parameters accordingly.
- Members of staff with distinctive surnames should be aware that it will be relatively easy for pupils to track them down on Facebook i.e. due to the large number of people named John Smith it is difficult to trace a specific individual.
- Members of staff should note that although these measures will make it harder for pupils to find them on Facebook a determined individual with knowledge of how the website works will eventually be able to trace a person down (given enough time).

Action to be taken if a member of staff is contacted by a pupil.

There are two types of contact through Facebook:

1. A message
2. An invitation to be added to a persons "Friends list"

If a message from a pupil is received the following action should be taken:

1. **Do not reply to the message.** Replying to a message allows the recipient to view your profile in its entirety. This is also a way to circumvent the privacy settings on account.
2. A senior member of pastoral staff (eg Housemaster / Assistant Head) should be contacted at the earliest opportunity and informed of the incident.
3. Pastoral staff should then be asked to speak to the pupil on behalf of the member of staff who was contacted. The relevant Facebook correspondence should be made available to the pastoral staff dealing with the situation to aid in any investigation.
4. The pupil should be reminded of the School's ICT Acceptable Use policy and that contacting staff in this manner is inappropriate. A note for file and notification to parents should also be made.

If an invitation to a person's friends list is received the following action should be taken:

1. **Immediately reject the invitation.**
2. A senior member of staff (eg Housemaster / Assistant Head) should be contacted at the earliest opportunity and informed of the incident.
3. Pastoral staff should then be asked to speak to the pupil on behalf of the member of staff who was contacted. The relevant Facebook correspondence should be made available to the pastoral staff dealing with the situation to aid in any investigation.
4. Note that rejection of a "friend request" allows the sender to repeat the action; if this occurs the relevant members of pastoral staff should be made aware of this.
5. The pupil should be reminded of the School's ICT Acceptable Use policy and that contacting staff in this manner is inappropriate. A note for file and notification to parents should also be made.

E-Mail – Good Practice

The nature of the Highgate School site and the busy schedules led by all who work here mean that Email can be a vital tool of communication. However, it is not a for fostering positive face to face relationships with colleagues. Email should not be regarded as a replacement for formal meetings or more informal conversations on the telephone or at staff briefings, break or lunch. The aim of this brief guide is to provide some suggestions on the way that email can be used most effectively and to improve the experiences of all those who interact electronically.

Is it necessary?

People are busy. Your message may be one of tens or hundreds for a recipient to deal with depending on how busy they are, how many lessons they have taught that day, how many extra-curricular activities they have been organising. If they are receiving so many messages, what are the chances that they will read your message with great care, particularly if they perceive it to be only tangentially relevant to them? For many people, Email is fast becoming a chore not a vital tool of communication. Do not accelerate this process by contributing messages / information that could be broadcast or communicated in another, often more efficient, way.

Beware of Forwarding

Consider carefully the necessity of forwarding a message and to whom. Take great care with any attachments, even from senders well known to you. When forwarding, include a summary of what you are sending – tell the recipients what it is in a sentence or two. If it is worthwhile to forward, it's worth an extra moment of your time to summarise your reason for forwarding.

Dealing with Emotions

One of the attractions of Email communication is that it can be quick and simple. However, this can also be a weakness. When you are writing letters, the very nature of the activity forces you to think about your choice of language. You may even go through a draft or two – considering carefully the impact of your words on the reader. Emails are often drafted all too rapidly and immediately sent off. Emotions or nuances you may feel were obvious could be missed by the recipient or perhaps they may read into your message and pick up attitudes or meaning that you had no intention of conveying. Humour is notoriously tricky to convey appropriately via Email, even to people that you know well. Therefore, the following suggestions can be useful:

Don't Criticise

Never chastise or criticise someone via an electronic communication. Even well meaning and constructive criticism can hit home much harder on screen when you are not there to moderate the blow with body language, vocal tone and flexible response to the observed reaction. Even if you do not feel that you are criticising – perception of a message must always be carefully considered.

Cool Off

If you have something to get off your chest, write the Email message then save it. Let it lie for a few hours / a day then re-read it. In the meantime, circumstances may change or you may have an opportunity to talk to the person causing your anxiety. Even if little has changed, it is highly likely that you will edit or re-write your original Email and it will be a more effective message for the greater sense of detachment and objectivity the extra reflection time has provided. Get out of the habit of a quick send then lengthy regret.

Take Care

Before responding to any Email message, re-read it to ensure that you fully understand it. Many messages are sent / forwarded without the reader really grasping the point and responding appropriately. Try to get into the habit of proof reading your own messages. This will ensure that your meaning and your requirements are clear and should help to minimise the chance of misunderstanding or frustratingly irrelevant replies.

Writing the Email

Clear entries in the *subject* guides to assist the reader in prioritising their inbox and sharp, concise email messages all play their part in making the process efficient and painless. Avoid putting too much information into one message – your key points may become buried. Email is, by its very nature, designed for short, digestible snippets of information. Readers do not expect tomes and they do not expect additional information beyond the subject guide. If you have lots to say then it may be lost in a long message – consider breaking it down into several messages or communicating your concerns in a different fashion.

Urgency and Reliability

Email feels immediate. It is not. It is subject to both technical system and reader variables. All staff should try to check their Email twice a day but, as we all know, sometimes this is not possible. Even when it does happen it is most likely to occur at 8a.m., lunchtime or after 4p.m. Bear this in mind when you send a message in the hope of a speedy reply by return. Try the phone. If it is urgent, check staff timetables and seek people out.

Email Conversations

If your email exchange on one topic results in two or more “cycles” then it is probably best to stop and talk to each other. Email will simply take too long and the subject is obviously knotty / complex enough to need a proper form of exchange with much more interactive feedback.

Email communication to parents should always be discussed with Housemasters in advance of any reply and a record of the exchange placed on the pupil’s file. If in doubt about any other external contact – speak to a member of SMT.

Appendix – 3 – Technology Policy Overview

This is located in all ICT suites and pupil's house rooms.

Technology Policy Overview for Pupils

This overview highlights key areas. For more details please refer to the ICT Acceptable Use Policy available on the intranet and in each of the computer labs.

- With the exception of portable computers, ICT equipment should not be moved, relocated or adjusted without the permission of a member of staff.
- Smartboards and Projectors should not be touched without a member of staff present in the classroom in order to supervise.
- With the exception of Sixth Formers using their personal laptops, pupils are not allowed to connect any personal devices to the network (wireless or cabled)
- No software should be installed onto any computer at School.
- If you accidentally damage or find damaged ICT equipment, please report it to the ICT department or a member of staff immediately.
- Internet access is provided for educational, research and personal development use. If pupils abuse this by seeking out sites that do not meet these objectives, they may be subject to appropriate disciplinary sanctions. Use of the School network is carefully monitored and recorded.
- Every pupil has a Home Space area to store private files and folders. If your work is important please save additional copies elsewhere as the School cannot guarantee against possible hardware failure. In order to maintain the efficiency of the system network administrators can, if necessary, gain access to your Home Space. Therefore do not store any personal photos, music or documents as your Home Space is designated for school work only.
- Any deliberate attempt to damage or 'hack' into the School's ICT infrastructure will result in serious disciplinary action that may include temporary or permanent exclusion from School.
- The use of mobile phones, iPhones and any music device in lessons (or in the transition period between lessons) is not allowed.
- Highgate School uses web filtering software to secure, monitor and limit certain websites for your security. However, if you feel that we have blocked a legitimate website then please let the ICT department know

Cyber-bullying

- The School regards cyber-bullying, through the inappropriate use of electronic communication such as text messages, email or postings on social networking websites like Facebook, as an unacceptable form of bullying. This includes the use of technology outside of normal School hours if it interferes with the safety and well-

being of any member of the School community. Such incidents will be treated seriously, investigated thoroughly and appropriate disciplinary measures taken if necessary.