MILLFIELD

ICT Acceptable Use Policy (AUP) Staff

Millfield School is committed to protecting its organisational interests by ensuring that its Information and Communication facilities processing systems are used in an appropriate manner.

The Heads of Millfield Schools

MILLFIELD

ICT Acceptable Use Policy (AUP) Staff

1 Purpose and aims of the AUP

Throughout this document 'Millfield ICT facilities' refers to the hardware, network infrastructure, software, ICT systems, data, and portable devices used at Millfield Senior School, Millfield Prep school, within boarding houses and used off site. 'Millfield School' refers to Millfield Senior School, Millfield Prep School, boarding facilities and any other part of the Millfield School organisation. Heads and SMT refer, as relevant, to Millfield Senior School and Millfield Prep School.

Staff must take reasonable steps necessary to ensure compliance with this, and other related policies.

This policy has been written and issued to:

- Promote the ethical, lawful and productive use of Millfield ICT facilities
- Define and prohibit unacceptable use of Millfield ICT facilities
- Educate users about their responsibilities
- Describe where and why monitoring takes place
- Outline disciplinary procedures

2 Who the policy applies to

The policy applies to the use of:

- Millfield ICT devices and any networks connecting them.
- all computer hardware owned, leased, rented or otherwise provided by a member of staff and connected to or otherwise accessing School networks or other school provided facilities
- such users include:
    - All employees
    - Boarding House and on-site families
    - Temporary staff
    - Voluntary staff
    - Employees of partner organisations
    - Contractors and subcontractors
    - Agents
    - Work experience placements
    - Other authorised temporary users, including work placements and visiting course members

3 Personal use

Millfield School recognises that access to Millfield ICT facilities for personal use can help employees to maintain a positive work-life balance:

Limited and 'reasonable' personal use of Millfield ICT facilities is permitted within the boundaries of reasonable use detailed below.

Internet access for personal use has been provided at risk and cost to the organisation. Millfield School asks that users make sensible and conscientious use of these facilities in return.

Occasional printing for personal use is permitted, but this should be limited to a few sheets only and in exceptional circumstances. Millfield Printing facilities must not be used as a substitute for routine home printing.

The operation of Millfield ICT facilities is logged and may be monitored (see section 4) to ensure compliance with this policy. Users that choose to make personal use of Millfield ICT facilities do so in the acceptance of the monitoring measures outlined in this policy.

Millfield School cannot guarantee security or accept responsibility if you choose to use personal data or undertake personal transactions using Millfield ICT facilities.

You are responsible for any personal activity conducted via your logon account.

Personal use of these facilities is a privilege. Millfield School reserves the right to withdraw such facilities either individually or globally at any time without notice or explanation.

Reasonable Use:

- Is lawful, ethical and complies with Data Protection and related Millfield policies
- Is in accordance with this policy
- Takes place during authorised breaks, non-contact periods or outside of working hours
- Does not adversely affect your productivity, or interfere with teaching & learning activity
- Does not make unreasonable use of limited Millfield resources

Unreasonable Use:

- Sending, viewing, or downloading of material that others might find offensive
- Sending, viewing, or downloading of unauthorised software
- Sending, viewing, or downloading of gambling content
- Unauthorised duplicating of material covered by copyright
- Personal use that can reasonably be described as excessive within the context of a professional working environment
- For commercial business use other than that of Millfield School and its associated interests
- Storing an unreasonable size of non-work related files/e-mails

It is good practice to mark any personal documents, folders, or communications as 'personal' whilst this doesn't guarantee privacy; it may avoid accidental viewing of such material.

4 Logging & Monitoring

Millfield School owns the organisation's' infrastructure, equipment, information systems, and any data that resides on such equipment. Millfield School has the right to log activity and use of such facilities at any time within the conditions set out below. Logging and monitoring is conducted to protect the organisation's' interests and to protect individual users. This must be done in a way that is both lawful and fair to staff, and if excessive and unjustified is likely to breach Data Protection laws. Under Data Protection laws, except under extreme circumstances, you have the right to know what logging and monitoring is taking place, why it is being carried out, who is collecting the information, who can view it, and how it will be used.

What is being routinely logged

- All Internet use is logged by display date, time, username and target URL (address of website being visited)
- All attempts to access blocked sites by displaying date, time, username and target URL

- Top Internet users, calculated by highest browse time
- E-mail accounts and folders logged by displaying file size
- E-mail use logged by displaying date, time, username, and the address to which the message is being sent or received
- Network folders, logged by displaying folder sizes and dates
- Telephone call traffic, including print-outs of itemised telephone call details for billing purposes

Routine logging takes place to facilitate the smooth, efficient, and cost-effective running of ICT infrastructure and systems and to ensure compliance with policy. All such cases of routine logging should be summative in nature & not intrusive into privacy.

The School uses a third party to filter spam before emails arrive at Millfield. Once e-mails and their attachments arrive at Millfield, they are routinely monitored by a scanning utility to detect the transmission or receipt of indecent or inappropriate images. Any emails alerted by such scanning are copied to the Network Manager and if found to be contravening School policy will be alerted to the Heads/Bursar.

How is such routine logging taking place?

- By software systems & utilities appropriate to the log

What is not being routinely logged?

- Screen viewing/capture*
- Web page content*
- Content of network files*

*Staff should be aware that such monitoring may take place under the direct and explicit instruction of the Heads/Bursar and only where serious and sufficient grounds of misconduct are suspected. Such items may also be viewed by technical support staff where a user has requested support and such viewing by ICT Support staff is necessary to remedy the problem and is agreed by the user.

Where monitoring has been permitted by the Heads/Bursar for cases where serious and sufficient grounds of misconduct is suspected, such monitoring will be conducted by the designated ICT Manager at the direction of the Heads/Bursar. Such monitoring will remain confidential to those staff authorised by the Heads/Bursar to undertake such activities. The users' line manager may be informed at the discretion of the Heads/Bursar.

Appropriate action regarding issues of misconduct is to be taken by the Heads/Bursar.

What covert monitoring can take place?

- Covert monitoring (where a staff member is not notified that monitoring is taking place) is not permitted except for some extreme circumstances such as investigating criminal activity. Such covert monitoring must be directly authorised by the Heads/Bursar and strictly targeted at obtaining evidence within a set timeframe, and within the boundaries of the suspected criminal activity. It must not continue after the investigation is complete, and that any other information collected during this time should be disregarded.

5 Enforcement of policy

Breach of this policy may invoke suspension of access to Millfield ICT facilities, and could at the discretion of the Heads/Bursar invoke the organisation's disciplinary processes. Breaches of this policy will be reported by the ICT & Communications Department to the Heads/Bursar, whereupon the schools disciplinary code may be implemented.

Serious and/or persistent breaches may constitute gross misconduct and could result in dismissal.

6 The Laws

All users are governed by current applicable UK law and any subsequent revision or additional laws; these include but are not limited to:

- Computer Misuse Act 1990
- The Communications Act 2003
- Data Protection Act 1998
- Copyright, Designs and Patents Act 1988
- Display Screen Equipment Regulations

You are personally responsible for ensuring that your use of Millfield ICT facilities is lawful. Failure to do so may result in disciplinary procedures outlined in the 'enforcement' section 5. You could also be liable to civil and/or criminal prosecution and/or claims for damages.

7 Security when using ICT systems & facilities

Complying with security procedures when using Millfield ICT is essential in order to protect both the user and the organisation. User logons and passwords permit access to sensitive and confidential data & systems.

The following security instructions must be implemented by each user:

- You are responsible for all the activity carried out via your logon & password
- Change your password frequently (press CTRL + ALT + DEL)
- Select a password which is not easy to guess
- Select a password that includes a combination of letters, numbers, & punctuation symbols
- If you have a portable device, comply with the policy within Section 8
- Lock your workstation or logout whenever it is left unattended
- Do not disclose your password to any other person
- Do not write down your password
- Do not let family members use or see your Millfield account or content viewed via your account
- If you suspect that your logon & password is being used by another person, change your password and report the incident to ICT Support immediately.

If logging on to Millfield ICT systems remotely or via a web portal, the same care and attention to security must be given.

Attempting to access or amend, or actually accessing or amending data and systems that you have not been granted access or authority to use, contravenes the Computer Misuse Act 1990.

To assist with workflow, network folders and school email accounts may be shared between staff, eg. managers and secretaries as long as both parties are in agreement.

In line with their duties, the IT Support and Network Support staff have access to all school email and network folders. This access is only permitted when requested by the owner or in line with Section 4 of this Policy.

8 Portable Devices

This policy applies at all times to any portable laptop, iPad, tablet, smartphone or other such mobile device used to access Millfield systems including email.

Devices issued to you by Millfield School remain the property of Millfield School and can be recalled for maintenance by ICT Support at any time. Portable devices are provided for business use and any personal use should not be significant. Limited and 'reasonable' personal use is permitted within the boundaries of reasonable use as set out in Section 3.

The same care with security and confidentiality of information should be taken as would be the case with ICT use within the school. Portable devices must be password protected and should be locked away when not in use. Portable devices should be left out of sight of thieves when in public places and cars.

Sensitive or confidential data, and data related to people protected under the Data Protection Act should remain on Millfield's secure and protected network drives. Users should avoid unnecessarily downloading sensitive or confidential information onto portable devices, or storage devices such as Flash memory sticks, CD's, DVD's or portable hard drives.

Any sensitive or confidential data, as identified through the Data Protection Act 1998, which is for whatever reason downloaded to a portable device or storage device must be encrypted using appropriate encryption software.

9 E-mail

Millfield School e-mail systems are provided for professional and business use only (however occasional personal correspondence is permitted in accordance with reasonable use detailed in section 3.)

- E-mail is not a secure method of communication; confidential information should not be communicated via e-mail. Communications could be accessed or modified by unauthorised individuals
- E-mail is admissible in court and carries the same weight as any other Millfield School written communication
- Once an e-mail message has been sent it is difficult and often impossible to retract it
- E-mail sent from the Millfield School e-mail system represents official communication from Millfield School and the same high professional standards and due caution should be given as with any other form of official Millfield written communication. Such e-mails directly represent Millfield School.
- Excessive or unnecessary e-mail communication hinders workplace efficiency
- The School reserves the right to access a staff e-mail account in the event of unexpected or prolonged absence, in order for the school to undertake that individual's job role

You must not:

- Open an attachment that you were not expecting
- Use your school e-mail account to register for goods or services that are non work-related
- Send inappropriate, confidential or sensitive information
- Send, forward or open anything that others may find offensive, obscene, discriminatory, defamatory, or contravenes copyright restrictions
- Provide banking, payment or personal details requested by e-mail unless you are sure of the authenticity of the message and sender
- Take part in or pass on any chain mail.
- Disclose information about a person that you would object to being disclosed about yourself

You must:

- Use the same care when writing an e-mail message as you would when writing a Millfield letter or memo
- Make sure that your message is concise, relevant, and sent only to the people who need to read it
- Use telephone or face to face contact instead of e-mail where this is possible and more appropriate
- Delete or archive old messages as appropriate from your e-mail account

10 Telephones

Telephones are provided for business use. To reduce costs, calls to mobile phones should be avoided where possible.

Millfield School recognises that using telephones for personal reasons can occasionally be necessary particularly in cases of emergency; however such use must be kept to a minimum. Normally personal mobile phones or public payphones should be used for personal non-work related calls.

Telephone traffic is logged and a quarterly statement of calls made via school telephones will be provided and members of staff are required to pay for any private usage.

School telephones must not be used for defamatory, abusive, obscene or otherwise inappropriate activity. Such breaches may invoke the schools' disciplinary procedures.

Where possible misuse is suspected, the length and destination of outgoing calls and source and length of incoming calls may be monitored.

Content of phone calls is not monitored unless under the direct and explicit instruction of the Heads/Bursar and only where serious and sufficient grounds of misconduct/criminal activity is suspected.

11 Use of the Internet & access to websites

Access to websites via the Internet is provided for business and professional use. Reasonable personal use of access to websites via the Internet is defined in section 3.

Millfield School logs all web access traffic to ensure proper compliance with this policy see section 4.

Access to certain sites may be blocked by filtering systems in order to protect you and Millfield School, this does not imply the suitability of sites that are accessible, and you must always use your professional discretion along with the guidance below when accessing websites. The guidance for parameters used for filtering is given by the SMT.

You must:

- Inform IT Support if there is a legitimate business or education-related site that you require unblocked via your logon
- For permanent unblocking of content for students, a request should be made in the first instance to IT Support who may refer to the Director of Academic ICT (Senior School)/Head of ICT (Prep school) for further consideration
- Inform IT Support if you believe that you have accidentally or inadvertently viewed or accessed inappropriate content

You must not:

- View, download or distribute anything that others may find offensive (racist, defamatory, pornographic, sexist, abusive, inciting hatred)
- Download or duplicate anything that contravenes copyright law (including images, music, software, animation, video)

- Upload information that contravenes section 12 of this policy
- Attempt to access 'high security risk' sites (including peer to peer file sharing sites, free software, warez, cracks, adult material, gambling) Further advice on this could be sought if required – see section 19
- Unnecessarily stream audio or video files that could adversely affect the performance of the network and normal school activity
- Attempt to circumvent the filtering system
- Contact pupils directly through sites that provide you with those means

12 Publishing information on public information systems

Student, staff and parental data is confidential and must be treated accordingly, and in line with the Data Protection Act 1998 and the School's Data Protection Policy and Guidelines.

Publishing school information on public information systems includes the submission of electronic content to web sites, e-mail, forums, blogs, wikis, and social networking sites. There is no control over who can read content published on public information systems, and such content cannot be deleted. It is important, therefore, that staff refer to Millfield's Social Media Policy. Staff should inform the Marketing Department if they suspect that school information has been published unofficially on public information systems.

13 Software legality

Installation and use of software, including apps, must comply with legal, contractual and licensing agreements.

14 Data protection legality

All users must comply with the Data Protection Act 1998 and the School's Data Protection Policy and Guidelines. If there is doubt over the compliance with such legislation the school's nominated Data Protection representative should be contacted for clarification.

In general terms, data about people 'data subjects' (including staff, pupils, clients, customers, parents, and associates) must be kept secure, must not be kept for longer than is necessary, must be accurate, and must be appropriate for the intended purpose.

15 Copyright legality

Copyright of all digital media including documents, images, video, animation, sound, software must be respected. If clarification of compliance is required please consult the appropriate School copyright licence and agreements.

Material displayed on the Internet may be subject to copyright restrictions which should be respected. Breaking copyright law occurs when a piece of work that is protected by copyright is reproduced. This includes music files, CDs and DVDs.

Many organisations presenting information over the Internet have become sensitive to breaches of their copyrights and have taken action against the perpetrators.

Contrary to popular belief, Web pages are not automatically in the public domain and are subject to the same usage restrictions as printed material. Unless you are absolutely sure that the author of materials displayed on the Internet has given permission to use their work, it should not be copied. Where an author does provide permission for taking copies for personal use, their restrictions on usage must be followed.

In no circumstances should materials copied from the Internet be included in Millfield Web pages or other publications, unless the copyright rules have been followed. In general terms, small amounts of copyrighted materials can be used in quotations and teaching resources provided that the source is stated. In other cases it may be necessary to obtain permission from the author for use of their material.

16 Health & Safety legality

Use of ICT equipment can pose health risks. It is your responsibility to seek clarification and advice on this issue from the Schools' nominated Health & Safety representative and understand school Health & Safety policies.

In general terms, staff should avoid eye-strain by taking regular breaks from viewing the screen, adjust keyboards, screens, and desk positions to prevent strain and promote good posture. Staff should ensure that adjustable chairs are adjusted to the correct position applicable to the user.

Care must be taken not to look directly into the beam of projection equipment – this applies to all users including students under your supervision.

17 Supervision of students & their use of ICT systems & facilities (e-safety)

There are real dangers posed to students during their use of information systems in a school environment. Whilst students are at school or in a boarding environment, their activity whilst using Millfield ICT facilities and their own personal ICT & communication equipment is the responsibility of the supervising member of staff.

Dangers include – grooming, bullying, defamation of character, fraud, identity theft, access to harmful or inappropriate websites. There is also a risk in terms of the student to student contact and interaction via ICT facilities.

Whilst using Millfield ICT systems, students' access to web sites and facilities is restricted using network controls and a filtering system, however no filtering system is 100% effective.

When students are accessing ICT facilities whilst under your supervision:

- Always closely supervise students activities where possible
- Be observant for misuse
- Serious concerns regarding the welfare/conduct of a student should be reported to the Head of Pastoral care/SMT as appropriate
- Make sure that students have logged off from their session
- Report any defects/damage/loss immediately to IT Support – this will help track & reduce vandalism etc.
- Do not allow a student to use a PC or laptop via a teacher logon or computer unless and only in the case of a directly supervised in-class demonstration using projection equipment or an appropriate supervised educational activity
- Do not leave your staff workstation logged on or unlocked when not in use by you.

18 Use of ICT facilities in Boarding Houses

For staff use and operation of ICT facilities in the Boarding House:

It is accepted that staff residing in a boarding house will have a greater requirement for personal use of ICT facilities. For this reason staff, their family members and visitors are issued with a 'family wireless key' where wireless is available. Those who use this facility must adhere to this Policy and other relevant School Policies.

Whilst boarding staff will not be able to monitor students' use of Millfield ICT facilities and students' own ICT facilities to the same level normally expected within school, vigilance and awareness of the issues raised in section 17 should always be applied where possible.

19 Where to obtain advice

Advice can be sought from:

- Your line manager
- IT & Communications Manager
- Director of Academic ICT (Senior school)/Head of ICT (Prep School)
- Designated Data Controller
- Health & Safety Representative
- Marketing Department
- Other applicable school policies

20 Acceptance of this policy

By using Millfield ICT facilities you agree to abide by this Policy and any subsequent revisions.

MILLFIELD

ICT Acceptable Use Policy (AUP) Staff

21 Version control

Revision of this policy will be notified to staff by e-mail, indicating the latest version number and where an electronic copy is stored and can be accessed. Staff must ensure that they are aware of and use the latest version. If in doubt please contact IT Support.

Document Title	Millfield School Information and Communication Systems Acceptable Use Policy (AUP)
Version	1.2
Status	Draft created for RDX/SMT approval
First Issued	Not yet released
Maintained by	BG/SCL

Version	Date	Details
1.0	13 Mar 09	Draft for SMT review – not reviewed
1.1	7 May 09	Draft updated. Commentary on IT & Systems Manager suggestions for change and reasoning for inclusion/rejection of items
1.2	2 Jun 09	Changes refined/agreed BG/SCL version submitted to RDX/SMT for approval
1.3	26 Aug 09	Final agreed by SMT
1.3a	31 Aug 11	Headmaster changed to Heads throughout document
1.3b	23 Apr 13	New Millfield logo in header
2.0	30 Jul 13	Update in line with Policy Reviews
2.1	8 Jan 14	Change to wording within Section 4 at request of the Audit Committee & change of title of document.