DATA HANDLING AND ELECTRONIC COMMUNICATION POLICY

Contents

Version History

Version	Status	Author	Date	Comments
1	Initial Draft	Gleeds	01/03/2012	Initial draft for discussion
2	First published	AGH	07/03/2012	For approval by DfE Pre-opening
3	First review	AJH	01/11/2014	First governors' review
4	Review	REA	15/10/2016	Governor's review

Review schedule: Annually, or as necessary, due to changes in relevant statutory legislation. (Education & ICT Sub Committee)

1. Introduction

1.1 Sandymoor School has a whole school data handling system designed to identify student potential and targets and then allow monitored intervention strategies to be put in place.

1.2 As electronic communications become faster, more powerful andeasier to use there is also, sadly, an increased risk of damage being caused through inappropriate use. This document also sets out how Sandymoor School seeks to ensure that its staff and pupils use electronic communications wisely.

1.3 The school processes a substantial amount of confidential and personal data and information on private individuals, employees, service partners and its own operation. This information is vital for the school to fulfil its role properly. Therefore the risks to its confidentiality, integrity and availability must be identified, quantified and mitigated.

1.4 The Data Handling and Electronic Communications Policy applies to everyone who uses school computer equipment, the school computer network or telephone systems including;

- Pupils of the school
- All employees of the school
- Others given access to the school's computer systems or information including partners, suppliers and other third parties.

1.5 All users must abide by the policy set out in this document at all times. In addition, users must use systems responsibly, comply with school requirements and operate within the law.

1.6 The policy applies to all equipment which facilitates electronic communications. This includes devices with computer-like functionality, which can manipulate information, and also to storage-only devices. These include, but are not restricted to;

- PCs and laptops
- Tablet PCs
- Electronic organisers
- Computer servers
- Digital cameras
- Scanners
- Telephones and faxes
- Mobile phones
- Two way radios (walkie-talkies)
- USB memory sticks
- CDs and DVDs
- External hard disks
- MP3 and MP4 players (including iPods)
- Network Connected Photocopiers

- Network connectivity devices e.g. modems and broadband devices
- Devices capable of wireless connectivity such as infrared and Bluetooth.

1.7 To be included in this policy a device does not have to be capable of manipulating the information it holds because all electronically stored information is capable of being inappropriately disclosed and of carrying malicious codes which could disrupt the school's computer network and systems.

1.8 This policy applies to all forms of data and information, which is owned by, administered or controlled by the school. This includes, but is not restricted to, text, still or moving images, maps, diagrams, video, audio, CCTV, music and sound recordings.

2. Risks of Electronic Communications

2.1 Misuse of the school's electronic communication facilities could expose both the school and individuals to the risk of legal claims against them including claims of defamation, discrimination or harassment, breach of copyright or contract, breach of the duty of confidentiality. It could even include criminal prosecution if child or violent pornography, materials promoting terrorism, racial, religious or sexual hatred, unlicensed software or unlicensed music files such as MP3s on the computer network is discovered, and criminal prosecution or civil action following a breach of data protection legislation.

2.2 In addition, misuse of the school's facilities could prejudice the availability and security of the school computers, computer network and the information held on or accessed through the computer network.

2.3 Such security breaches could potentially damage the school's reputation and lead to financial losses, distress, inconvenience, embarrassment, loss of information privacy, threats to personal safety, and crime.

2.4 Flexible working, where users work from home, presents additional risks to information as small computing equipment and storage devices are easily lost or stolen or connected to an insecure computer or network.

2.5 Therefore the School needs to set out rules of acceptable use of all forms of electronic communication, the consequences of misuse and the measures that will be taken to monitor compliance with the policy

3. Relevant Legislation

3.1 Both line managers and individuals have responsibilities regarding the legal use of electronic communications. There are now many laws and legal

rules governing information and data security and some examples are shown below.
3.2 Availability: The Freedom of Information Act 2000 seeks to ensure that information is disclosed to the public unless an existing prohibition on disclosure exists by way of statute or through the use of an available exemption available through the Freedom of Information Act.

3.3 Confidentiality: The Data Protection Act 1998 protects personal information from disclosure: an individual might commit a criminal offence by disclosing personal information without the authority of the organisation. Also there are duties of confidentiality under common law.

3.4 Integrity: The Data Protection Act 1998 requires that personal information is adequate, relevant, is not excessive and is accurate.

4. Breaches of the Data Handling and Electronic Communications Policy

4.1 Any unusual occurrence, which might indicate the presence of a computer virus, or a clear breach of security whilst using electronic communications, must be reported immediately to ICT Support.

4.2 The user's line manager should be notified immediately if any of the rules specified in this policy are broken inadvertently, in order to avoid or mitigate disciplinary action for breaching the policy.

4.3 Actions or neglect leading to a breach of this policy by an employee could result in disciplinary action.

4.4 Breaches of this policy by a user who is not a direct employee of the School may result in action being taken against the user or his or her employer.

5. General Requirements for All Users

5.1 This policy applies to all users, at all times and in all locations where Sandymoor School computer network or equipment is used, or school information is accessed.

5.2 Sandymoor School operates within the law at all times and the following points must be observed;

- Information must not be saved on the computer network or uploaded onto the Internet in breach of copyright
- Intellectual property rights and import / export regulations must not be breached
- All copies of computer software used must have a current licence the purchase of which must be auditable; the source of free and evaluation software must be documented

- Personal information must only be stored on the system if the purpose for which the data is held is covered by the school's notification under the Data Protection Act 1998
- The requirements of the Freedom of Information Act 2000 must be complied with.
- Confidential and personal information must be protected appropriately at all times and particularly when it is transmitted electronically outside the school or stored on mobile computing or storage devices
- Confidential and personal information must not be uploaded onto the Internet or any other network
- Confidential or personal information must not be displayed on an unattended PC screen
- Users must not attempt to access a system for which they have not been given authority
- Users must not deliberately access or use any form of malicious software
- Users shall not watch live television on any school owned device without management approval (managers must ensure that a valid television licence is held or is not required)
- Hand held mobile phones or any other devices must not be used to send or receive phone calls, texts, e-mails or to access the Internet whilst driving.

5.3 Electronic communications must not be used in any way that might be seen as inappropriate.

5.4 Electronic communications must not be used in any way that might be seen as defamatory, libellous, insulting or offensive by others, or in any way that contravenes any other Sandymoor School policies.

5.5 Communications must not contain material that is profane, obscene, indecent, pornographic, defamatory, inflammatory, threatening, discriminatory, harassing (racially, sexually or otherwise offensive), subversive or violent, racist or of an extreme political nature, or which incites violence, hatred or any illegal activity.

5.6 Only conventional and authorised routes to electronic communications facilities may be used.

5.7 Users must not interfere with the configuration of operating system software, including Internet Explorer or other Internet browsers, on PCs, laptops, network devices, phones or other devices.

5.8 Users shall not attempt to bypass or subvert school implemented system security controls, including the virus scanner or by installing any other software.

5.9 Software, including screen savers, must not be downloaded or installed

without approval from ICT Support.

5.10 Any macros used in office automation software such as Microsoft Office must be acquired from trusted sources e.g. written in-house. If in doubt, guidance should be sought from ICT Support.

5.11 When using School owned devices, access to the Internet must be made through using software and hardware provided for that purpose by ICT Support. Any exceptions to this must be formally risk-assessed and require approval by ICT Support.

E-mails must be sent via the school's e-mail system. Sending to and receiving mails from other users of web based accounts is allowed for business purposes, but must be considered less secure.

6. Controlling Access to computer and telephone facilities

6.1 In order to maintain full accountability, each user shall have an individual user name and password, which shall not be shared with others. Similarly, individual e-mail accounts shall not be shared with others.

6.2 Passwords used to access information or computing facilities must be kept **secret** and protected from disclosure whilst being typed. Any "Remember Password" feature, where passwords are stored in an automated logon routine, must not be used.

6.3 Strong passwords, which are difficult to guess, must be used. A unique password must be used each time the password is changed.

6.4 Passwords must be changed regularly wherever possible and changed immediately if it is suspected that someone else may have seen or guessed it. Wherever possible a password must be changed on first use when it has been set or reset by someone else, e.g. a system administrator or ICT Support.

6.5 Only **authorised** people are allowed to access the School's information, equipment or computer network; all PCs must be logged off or locked when unattended; computing equipment shall be positioned so that unauthorised people, including colleagues, are not able to view sensitive information; external visitors must be supervised appropriately at all times.

6.6 School equipment must not be passed to anyone else without management approval and without the School's asset register being updated. All users who are about to leave School employment must arrange for any mobile computing equipment and computer storage used to be returned to ICT Support before leaving.

6.7 All information shall be removed from all equipment before disposal. Only ICT Support approved methods of disposal shall be used.

7. Electronic communications are for business use

7.1 Electronic communications must not be used for personal gain or profit

7.2 Non-work related information must not be stored on the network servers, PCs, laptops or any other school-owned device without management permission.

8. General requirements

8.1 Computing hardware and software shall be purchased in negotiation with ICT Support. All hardware and software must be sourced from reputable suppliers to ensure that it cannot be used to introduce malicious code into the school's computers or computer network.

8.2 The physical security of all school equipment and information must be considered at all times and in all locations and adequate provision for secure storage of all equipment, including servers and network devices, must be made. Particular arrangements for physical security shall be made for premises outside school and when travelling.

8.3 Users shall seek management guidance before sensitive information and school owned equipment is removed from school premises to ensure that adequate security controls are in place.

8.4 Laptops and other portable devices, and all forms of information storage must be locked away when not in use; equipment shall never be left unattended in a viewable or accessible place.

8.5 Mobile equipment must not be left in an unattended vehicle even when it is parked at the user's home. Particular care must be taken to protect mobile phones and small mobile storage devices.

8.6 Users shall not interfere with or change physical security measures introduced by ICT Support that protect against theft, tampering and unauthorised use of equipment; users shall follow instructions and guidelines for their use.

8.7 Consideration must be given to the need for additional physical protection for critical information, such as storing in a fire and heat resistant safe when not in use.

8.8 ICT equipment, software or information that is lost or stolen should be notified to SLT as soon as possible.

8.9 Staff must make appropriate arrangements for their manager or other colleagues to access their School information (e.g. e-mails and voicemails) when they plan to be absent from work for a day or more.

8.10 Users are responsible for ensuring that backup copies are taken of important and essential information that they have created and are responsible for on PC hard drives and all mobile computer devices and storage. Users must remember that any information stored on a local PC hard drive or mobile computing device or storage is at risk of loss and may not be retrievable in case of system failure. Backup copies of information must be protected from unauthorised access, theft, and loss at all times, including at disposal.

9. Professional and courteous use of electronic communications

9.1 Users shall not use electronic communications in any way that could damage the School's reputation.

9.2 Users must not photograph or film by any means, including web cams and mobile phones, confidential information without management approval.

9.3 All information on electronic media (e.g. CDs) must be checked for malicious code before it is sent to other organisations using an up-to-date virus scanner on a PC or by asking ICT Support for assistance.

9.4 Users must not represent their own personal opinion as being that of Sandymoor School.

10. Use of the Telephone and Fax and Two-Way Radios

10.1 If confidential information is requested over the phone it must be disclosed only to authorised people. If asked for such information by phone, the user must check that the caller is who they say they are and that they are entitled to the information. Check any telephone or fax number given by the caller and call back with the information.

10.2 Exercise caution when talking on the phone. Confidential and personal information must be protected from eavesdropping during telephone conversations and when listening to voicemail messages or answering machines, by choosing a suitably private environment. Voicemail messages must not be listened to on a speakerphone unless the user is in a private office.

10.3 The voicemail password on all School voicemail accounts must be changed on first use.

10.4 Do not leave sensitive messages on voicemail or answering machines.

10.5 Fax machines where confidential or personal information may be received must be sited in a secure area or attended until the fax arrives. Confidential incoming faxes must be delivered directly to the recipient or put in a sealed envelope marked confidential before distribution.

10.6 Confidential or personal information to be faxed must be labelled appropriately and must be sent to a fax machine in a secure area and/or where the recipient will be waiting by the fax machine. Care must be taken that the fax is sent to the right phone number and confirmation of delivery should be requested. Note that the information in the fax may be retained in the internal message store on some fax machines.

10.7 Conversations held on two-way radios are easily intercepted on another radio using the same channel and confidential information must not be disclosed when using them. If there is reason to believe that transmission is being intercepted, an alternative channel must be selected.

11. Use of the Computer Network

11.1 The computer network must be protected at all times. Any PC, laptop, telephone, camera or other device, e.g. a PDA, which has been connected to another network, must not be connected to the school computer network without first being examined and approval granted by ICT support before connection to the school network.

11.2 Another network includes a home PC, another company's or partner's private network, a wireless or phone network or the Internet and any device which itself is ever connected to another network; this includes connection of a PDA to a home PC

11.3 Personally owned equipment and storage devices must not be connected to the School computer network or to any School-owned equipment, whether on the School's network or not.

11.4 ICT Support reserve the right to enforce this policy by disconnecting and removing equipment, including Non-School or personally owned equipment that has been attached to the School's computer network.

12. Non-School or personally owned equipment/storage devices

12.1 Non-School equipment shall not be connected to the computer network without permission from ICT Support.

12.2 All information entering the School network or onto School computer equipment, by any means and from whatever source, must be checked for malicious code such as viruses and worms; this includes mobile storage devices such as CDs, USB memory sticks and external hard disks.

12.3 Users shall not use modems and other network attachment devices without permission from ICT Support.

13. Devices with wireless capability

13.1 Devices with any type of wireless capability e.g. Bluetooth, which are ever connected to school's computer network, must have this facility switched off at all times, even when not connected to the school's computer network, unless permission from ICT Support has been obtained.

13.2 If there is an agreed business need for the use of Bluetooth hands-free with a mobile phone that is ever connected to the school computer network, this must be set up by ICT Support to ensure that it is done securely. It is the user's responsibility to ensure compliance with any other School policy related to the use of mobile phones.

13.3 Wireless access points of any type must not be connected to the school's computer network without written permission from ICT Support.

14. Anti Virus and security patches

14.1 All information must be scanned for malicious code before entering the school network.

14.2 All PCs, laptops, PDAs and other devices must have up-to-date virus checking software, either downloaded from the network or manually applied if stand-alone. Users must ensure that **all** updates to virus checking software are applied as soon as possible.

14.3 Laptops and other mobile devices must be made available to ICT Support for applying security patches when requested.

15. Use of E-mail

15.1 Users shall always check that the intended recipients of e-mail messages are correctly identified so that sensitive information is not accidentally released to unauthorised users.

15.2 E-mail headers or message contents must not be changed when forwarding e-mails so as to misrepresent the views of others**; be aware that others may change e-mails written by you or forwarded to you**. Copies of important e-mails sent must be kept.

15.3 E-mails must not be automatically forwarded to an e-mail address outside of the school without protection from interception, e.g. by use of encryption.

15.4 Passwords must not be included in the text of an e-mail that refers to an attachment, which is password protected because it contains confidential or personal information. Password protecting attachment offers only very limited protection and alternative means of protection, such as encryption, must be used to protect information which is sensitive or confidential.

15.5 All external e-mail and attachments, incoming and outgoing, must be scanned for malicious content.

15.6 Whilst every effort is made to block e-mails containing undesirable material, it is possible that some will still get through and all e-mail users must accept that this may be the case.

15.7 Users must not create or forward an e-mail chain letter or chain text message.

15.8 "Phishing" e-mails requesting personal information such as credit card details, user names and passwords, or containing links to Internet sites where such information is requested, must always be ignored and deleted.

15.9 Extreme care must be taken in opening attachments of external e-mails if they are not expected and are not from a known and reliable source. ICT Support can provide advice if it there is concern that an e-mail or attachment might contain a virus or other malicious code.

15.10 E-mails warning of viruses and other malicious code must be forwarded immediately to the ICT support. Do not follow instructions in such mails unless they are issued by ICT support, because they might be a hoax.

16. Use of Internet

16.1 Information on the Internet must be treated with caution due to the unregulated nature of public networks.

16.2 Use of on-line chat rooms, Instant Messaging, on-line computer games and gambling on-line is forbidden.

16.3 Text or images, which contain anything that may bring the school into disrepute, must not be loaded on to the Internet.

16.4 Illegal or inappropriate Internet sites must not be accessed and will be blocked wherever possible.

16.5 ICT Support should be contacted when access to blocked Internet sites is essential for business reasons.

16.6 Care must be taken when opening or downloading files from the Internet if they are not from a known and reliable source.

16.7 All internet activity logged to a user name will be deemed to have been performed by them.

17. Flexible Working

17.1 A user shall obtain authorisation from his or her line manager before using mobile computing equipment to process, store, or access school information. Users should seek advice from their line manager as to whether highly sensitive information may be accessed whilst in places accessible to unauthorised users, e.g. whilst travelling by public transport.

17.2 Removable media devices such as USB memory sticks, CDs and DVDs should be used only where there is a business requirement and where no network connection is available or practical.

17.3 Allowing the use of removable media devices increases significantly the risk of malicious software being introduced and of information being inappropriately disclosed.

17.4 Sensitive or personal information must not be put onto non-school equipment without written management permission. If such information is stored on a home PC, the information must be professionally removed (not just deleted) or the disk physically destroyed before disposal of the home PC.

17.5 All mobile computing devices and mobile storage devices must be capable of being password or PIN protected and this must be enabled on all mobile devices. Wherever possible, passwords of at least 6 and preferably 8 characters long should be used.

17.6 All users must be advised how to create strong passwords. Biometric access control shall be considered where the information stored warrants more secure authentication.

17.7 Users should notify ICT Support at the earliest possible opportunity if they experience an operational problem with School owned mobile computing facilities or equipment and arrange for affected equipment to be inspected by ICT Support if required.

18. Encryption Policy

18.1 Encryption is a means of scrambling information so that only authorised people with the correct key can read it. This encryption policy applies to all types of mobile devices which contain computer readable information storage.

(Note that to be included in this policy such a device does not have to be capable of manipulating the information it holds because all electronically stored information is capable of being inappropriately disclosed and of carrying malicious code).

18.2 This policy includes devices with computer-like functionality, which can manipulate information, and also to storage only devices. These include, but are not restricted to;

- Laptops

- Tablet PCs
- Mobile & "smart" phones
- Digital cameras
- MP3 and MP4 players
- USB memory sticks
- Tapes, CDs and DVDs
- External hard disks.

18.3 Wherever technically feasible, encryption software shall be installed on **all** new mobile devices. ICT Support will decide if encryption software is technically feasible. Where encryption software is not technically feasible, an individual information risk assessment must be completed to determine if it is acceptable to store the information unencrypted.

18.4 All information held on existing mobile devices shall be assessed for its need for confidentiality. With the proviso regarding technical feasibility detailed above, encryption of information on mobile devices and storage is mandatory in the following situations;

- The information held is defined as "**personal**" or "**sensitive**" under the Data Protection Act 1998
- The information held is **commercially sensitive**
- Where any of the information held might be **prejudicial** to the School's reputation were it to be inadvertently disclosed
- The device or storage contains e-mails. This is because e-mails often contain information classified as "**personal**" under the Data Protection Act 1998 and the user has no control over the content of e-mails sent to him or her.

18.5 ICT Support shall evaluate and provide standard encryption products for each type of mobile device and each level of security required. All encryption products used must be approved by ICT Support.

18.6 Where information is of a particularly sensitive nature, a more robust encryption product shall be considered - this is one that has been independently and formally evaluated against government defined security criteria.

18.7 Under normal circumstances all confidential, sensitive and personal information should be stored on network servers, however in exceptional circumstances if such information is kept on desktops, an exception to policy would be required by completing a risk assessment and ensuring the PC has full disk encryption.

18.8 The School retains the right to decrypt and examine all encrypted information on School devices. Encryption/decryption keys must be stored securely by the line manager and must be made available to ICT Support on request

19. Reporting Security Incidents and Software Malfunctions

19.1 An event that causes loss or damage to school information, or an action that is in breach of any school security policy, including this policy, should be reported immediately.

19.2 Users shall immediately notify their line managers and ICT Support of any suspected or actual security incidents, weaknesses or software malfunctions, i.e. any event that causes, or could cause, loss or damage to school information, or an action that is in breach of any School security policy, including this policy.

19.3 Evidence associated with a security incident must not be tampered with or deleted until authorised by the user's line manager or ICT Support. Under no circumstances should an attempt be made to replicate or simulate any suspected security threat or weakness, as the attempt could be deemed as misuse of the computer system.

19.4 Users must not attempt to correct a software malfunction by for example, removing the suspected software or by changing any software settings within or outside the software package. The user must immediately seek advice from the ICT Support. Any portable media such as diskettes or CDs used on the affected computer must not be used on any other computer to ensure the software malfunction is not inadvertently spread to other computers or the computer network.

19.5 Suspected malicious software must be reported immediately to ICT Support by telephone (not e-mail), and work ceased on the PC or other device.

20. Personal Use of the Internet

20.1 Users are trusted to use the Internet responsibly recognising that School business is a priority and that the network must be protected from unreasonable and excessive personal use. Managers are responsible for ensuring that all users understand that this is a condition of allowing personal use.

20.2 If personal use of the Internet causes problems with business access, personal use might be withdrawn. All conditions of use in this policy must be complied with during personal use and some of the key ones are repeated here for emphasis.

20.3 The School provides ICT facilities for School business. **Small** amounts of personal use of the Internet is allowed in **non-work time** where there is no effect on the performance, effectiveness or timekeeping of the individual in performing their duties and no impact on others' business use of the Internet.

20.4 ICT Support provides support for business use and it must **not** be contacted for queries concerning personal use of the Internet.

20.5 The Internet must not be used in any way that might be seen as defamatory, libellous, insulting or offensive by others, or in any way that contravenes any school policies. Communications must not contain material that is profane, obscene, indecent, pornographic, defamatory, inflammatory, threatening, discriminatory, harassing (racially, sexually or otherwise offensive), subversive or violent, racist or of an extreme political nature, or which incites violence, hatred or any illegal activity. Harassment is defined in the school policy on Anti-bullying.

20.6 The school accepts no responsibility or liability whatsoever for problems of any kind caused to or by users arising from personal use, for example (but not limited to) when buying goods online, including identity theft and compromise of credit card numbers.

20.7 All users are responsible for reducing the risk of downloading malicious code, such as viruses and spyware (code that is secretly installed and can be used to steal bank or credit card details). To do this all users must check that the anti-virus software on their PC is kept up to date either automatically for desktop PCs or on laptops by requesting an update when connected to the network. Whilst the anti-virus software should be updated automatically on desktop PCs, now it is important that this is checked regularly.

20.8 Some web sites are more likely to contain malicious code than others. It is very difficult to provide specific guidance on this but large reputable companies and organisations make every effort to protect their web sites from malicious code. Users are expected to use their common sense to keep the risk of malicious code to a minimum. If a PC malfunctions in any way, this must be reported to the ICT Support immediately because it might be an indication of infection by malicious code.

20.9 Personal information, bank details, usernames and passwords must **not** be included in an automated log on routine, e.g. where there is a check box to “remember password?” this must **not** be checked. If this were done, another user on the same PC might be able to gain access to personal banking or other accounts.

20.10 The downloading of video, music or online games for personal use is not allowed. Non-work related data must not be stored on the network servers without management permission and anything downloaded must be legal. Large volumes of information for personal use must not be downloaded from the Internet as it might impact on Internet performance for business use.

20.11 Inappropriate Internet sites will be blocked wherever possible.

20.12 The Internet must not be used for personal gain or profit.

20.13 Privacy of any communications cannot be guaranteed. All monitoring will be fair and proportionate to the risks of harm to the School's reputation and the information stored on the system, and undertaken so as to intrude on users' privacy only as much as is necessary.

20.14 Users are reminded that actions or neglect leading to a breach of this policy by an employee could result in disciplinary action; this could include dismissal without notice even for a first offence if sufficiently serious. Breaches of this policy by a user who is not a direct employee of the School may result in action being taken against the user or his or her employer.

21. Monitoring of this Policy

Monitoring of this policy will be;

21.1 To ensure that this policy is adhered to and to detect and investigate unauthorised use of electronic communications.

22.2 To maintain the effectiveness, integrity and security of the network.

22.3 To ensure that the law is not being contravened.

22.4 To protect the integrity and reputation of the School and the services it provides.

22.5 All monitoring will be fair and proportionate to the risks of harm to the school's reputation and the information stored on the system.

22.6 Undertaken so as to intrude on users' privacy only as much as is necessary.

22.7 Carried out similarly regardless of whether the user is office based or working remotely.

22.8 Carried out subject to the requirements of legislation. Access to any records of usage will be stringently controlled.

23. Suspected misuse of the school's equipment, network and/or breaching this policy

23.1 Where the school has received a complaint or reasonably suspects that a user is misusing the school's equipment, network and/or is breaching this policy, any school owned equipment processing electronic information, and the content of mobile storage device such as diskettes, CDs and USB memory sticks, may be examined by appropriate management and/or ICT Support.

23.2 All school hardware and software remains the school's property at all times and must be made available for inspection immediately upon request.