St Monica's R.C. High School and Sixth Form Centre E safety and Acceptable Use Policy

September 2016

MISSION STATEMENT

St. Monica's is a Catholic community working in partnership with families, schools and parishes to teach the Catholic faith as a way of life. We provide a caring, supportive environment where everyone is of equal worth. Jesus Christ is central to our school and our main aim is that everyone can develop their God given talents and gifts to the full, while growing in faith through prayer and service.

Introduction and Aims

The purpose of this policy is to establish the ground rules we have in school for using ICT equipment and the Internet.

New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. The Internet and other digital/information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times. The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This e-safety policy will help to ensure safe and appropriate use. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to, loss of or sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/Internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is read and used in conjunction with other school policies; specifically Anti-Bullying, Model Professional Relations, Safeguarding and Child Protection

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

The school provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The e-safety policy explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

Scope

This policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents/carers and visitors) who have access to and are users of school IT systems, both in and out of school. The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may

take place out of school, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles & Responsibilities

This section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

Governors

Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy. The governor responsible for Safeguarding will also have responsibility for E-Safety.

They will discharge these duties by:

- Meeting with the ICT and E-Safety Coordinators
- Monitoring of filtering/change control logs

Senior Leadership Team (SLT)

The Head teacher is responsible for ensuring:

- The safety (including e-safety) of all members of the school community, although the day to day responsibility for e-safety may be delegated to the E-Safety Coordinator
- Adequate training is provided
- Effective monitoring systems are set up
- That relevant procedure in the event of an e-safety allegation are known and understood.
- Establishing and reviewing the school e-safety policies and documents (in conjunction with e-safety co-ordinator)
- The school's Designated Child Protection Officer (Mrs Walker) should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise through the use of IT.

E-Safety Coordinator

The E-Safety Coordinator takes day to day responsibility for e-safety issues and has a leading role in:

- Liaising with staff, (including the Designated Child Protection officer) the LA, ICT Technical staff, E-Safety Governor and SLT on all issues related to e-safety;
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- Providing training and advice for staff;
- Receiving reports of e-safety incidents and creating a log of incidents to inform future e-safety developments;
- Co-ordinating and reviewing the e-safety education programme in school

ICT Coordinator

The ICT Coordinator is responsible for ensuring that:

- The school's ICT infrastructure is secure and meets e-safety technical requirements
- The school's password policy is adhered to
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Co-ordinator keeps up to date with e-safety technical information

- The use of the school's ICT infrastructure (network, remote access, e-mail, VLE etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Coordinator and/or SLT for investigation/action/sanction.

The ICT Coordinator has a responsibility to ensure that the I.T. support team adhere to the above e-safety measures during the course of their activities and are aware of Security and Acceptable Usage Policy.

Teaching & Support Staff

In addition to elements covered in the Staff Accessible Usage Policy (AUP), all teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read and understood the school Safeguarding policies and procedures, and signed the school Safeguarding document.
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils/students understand and follow the school's e-safety and acceptable usage policies
- Pupils/students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended school activities
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

Pupils (to an age appropriate level)

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Usage Policy, which they will be required to sign before being given access to school systems. (this is to be found in the school journal.) Parents/carers will also be required to read through and sign an internet permission form in the school journal. Pupils will not be allowed to access the school systems without this.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy also covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take opportunities to help parents understand these issues. Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Usage Policy.
- Accessing the school website in accordance with the relevant school Acceptable Usage Policy.

<u>Education and Training</u>

E-safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of the assembly programme and is regularly revisited in Information Technology and other lessons across the curriculum – this programme covers both the use of ICT and new technologies in school and outside of school.

- Pupils/students are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Pupils/students are encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school.
- Pupils/students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Rules for the use of ICT systems and the Internet are posted in school
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

Acceptable Usage Policy (see Appendix 5/6)

- **Parents/carers** will be required to read through and sign alongside their child's signature, helping to ensure their children understand the rules

Copyright

- Pupils/students to be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations- staff to monitor this.
- Pupils/students are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.

Staff Training

- E-safety coordinator ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- All new **staff** receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy, Acceptable Usage and Child Protection Policies.
- The **E-Safety Coordinator/SLT link** will receive regular updates through Local Authority and/or other information/training sessions and by reviewing guidance documents released.
- **Governors** are invited to take part in e-safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, e-safety, health and safety or child protection.

Communication

Email

- Digital communications with pupils should be on a professional level and only carried out using official school systems (see staff guidance in Model Professional Relations Policy).
- The school's e-mail service should be accessed via the provided web-based interface by default (this is how it is set up for the laptops, school curriculum systems);
- Under no circumstances should staff contact current pupils/students, parents/carers or conduct any school business using personal e-mail addresses. Staff should not contact former pupils/students under the age of 18 via personal email.
- School e-mail is not to be used for personal use. Staff can use their own email in school (before, after school and during lunchtimes when not working with children) – but not for contact with parents/ pupils.

Mobile Phones

- **School** mobile phones only should be used to contact parents/carers/pupils//students when on school business with pupils/students off site. Staff should not use personal mobile devices.

- **Staff** should not be using personal mobile phones in school during working hours when in contact with children.
- **Pupils** should adhere to the rules and guidelines set out in the Behaviour Policy regarding mobile phone use in school.

Social Networking Sites

Young people will not be allowed on social networking sites at school; at home it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.

- **Staff** should not access social networking sites on school equipment in school or at home. Staff should access sites using personal equipment.
- **Staff** Should not be in contact with any current pupils or students, or former pupils/students under the age of 18 via social media. If any staff have children at the school they should let the designated person know to discuss the implications of being linked on social media.
- **Staff** users should not reveal names of staff, pupils, parents/carers or any other member of the school community on any social networking site or blog**.**
- **Pupils/students/parents/carers** should be aware the school will investigate misuse of social networking if it impacts on the well-being of other pupils/students or stakeholders.
- If inappropriate comments are placed on social networking sites about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary. If staff or pupils are found to have posted such comments they will also be dealt with through the school disciplinary processes for staff and pupils.
- **Pupils** in the KS3 curriculum will be taught about e-safety on social networking sites as we accept some may use it outside of school.

Digital Images

- The school record of parental permissions granted/not granted must be adhered to when taking images of our pupils/students. The list is available from SIMS.
- Under no circumstances should images be taken using privately owned equipment without the express permission of the Head teacher, a member of SLT or the ICT co-ordinator.
- Where permission is granted the images should be transferred to school storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity.
- Permission to use images of all staff who work at the school must be sought before being used.
- Images of children being posted online should not have the pupils' names on.

Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. The school has an active website and twitter account which are used to inform, publicise school events and celebrate and share the achievement of pupils/students.

Removable Data Storage Devices

- All files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using school provided anti-virus software before run, opened or copied/moved on to local/network hard disks.

Websites

- In lessons where Internet use is pre-planned, pupils/students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Staff will preview any recommended sites before use.
- "Open" searches (e.g. "find images/ information on...") are discouraged when working with younger pupils who may misinterpret information.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. **Parents/Carers** will be advised to supervise any further research.
- **All** users must observe copyright of materials published on the Internet.
- Teachers will carry out a risk assessment regarding which pupils/students are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the pupils/students on the internet by the member of staff setting the task. All staff are aware that if they pass pupils/students working on the internet that they have a role in checking what is being viewed. Pupils/students are also aware that all internet use at school is tracked and logged.
- The school only allows the SLT to access to Internet logs with the express, written permission of the Headteacher.

Passwords

Staff

- Passwords or encryption keys should not be recorded on paper or in an unprotected file
- Passwords should be changed at least every 3 months
- Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems

Pupils/Students

- Should only let school staff know their in-school passwords.
- Inform staff immediately if passwords are traced or forgotten.

- **Use of Own Equipment**

- Privately owned ICT equipment should never be connected to the school's network without the specific permission of the Head teacher or ICT co-ordinator.
- Pupils/students should not bring in their own equipment unless asked to do so by a member of staff.

Use of School Equipment

- No personally owned applications or software packages should be installed on to school ICT equipment;
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.
- All should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

Monitoring

All use of the school's Internet access is logged. Whenever any inappropriate use is detected it will be followed up by the E-Safety Co-ordinator, Heads of Department, Heads of Year or members of the Senior Leadership Team depending on the severity of the incident.

- The E-Safety Coordinator and ICT Co-ordinator will maintain the Change Control Log and record any breaches, suspected or actual, of the filtering systems
- Any member of staff employed by the school who comes across an e-safety issue does not investigate any further but immediately reports it to the e-safety co-ordinator and impounds the equipment. This is part of the school safeguarding protocol. (If the concern involves the E-Safety co-ordinator then the member of staff should report the issue to the Head teacher).

Incident Reporting

Any e-safety incidents must immediately be reported to the Head teacher/designated person (if a member of staff) or the E-Safety Coordinator (if a pupil/student) who will investigate further following e-safety and safeguarding policies and guidance.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. Listed in Appendix 2 are the responses that will be made to any apparent or actual incidents of misuse. If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials, actions will be followed in accordance with policy, in particular the sections on reporting the incident to the police and the preservation of evidence. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows (Appendix 3 for pupils/students and Appendix 4 for staff respectively).

Appendix 1

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

		Staff and other adults					Pupils/Students			
Communication Technologies		Permitted	Permitted at certain times	Permitted for named staff	Not Permitted		Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
Mobile phones May be brought to school		✓						✓		
Mobile phones used in lessons					✓					✓
Use of mobile phones in social time		✓								✓

Taking photographs on mobile devices			✓				✓		
Use of PDAs and other educational mobile devices		✓				✓			
Use of school email for personal emails					✓				✓
Social use of chat rooms/facilities					✓				✓
Use of social network sites				✓					✓
Use of educational blogs		✓				✓			

*Named staff are those who have received training from the Social Media Co-ordinator.

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils/students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to SLT (in accordance with the school policy) the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers (email, text etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Pupils/students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Appendix 2

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows. Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					✓
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
Adult material that potentially breaches the Obscene Publications Act in the UK					✓
Criminally racist material in the UK					✓
Pornography					✓
Promotion of any kind of discrimination				✓	
Promotion of racial or religious hatred					✓
Threatening behaviour, including promotion of physical violence or mental harm					✓
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business				✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Bury Council and / or the school				✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				✓	
Creating or propagating computer viruses or other harmful files				✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				✓	
On-line gaming (educational)		✓			
On-line gaming (non- educational)				✓	
On-line gambling				✓	
On-line shopping / commerce			✓		
File sharing			✓		
Use of social networking sites				✓	
Downloading video broadcasting e.g. Youtube	✓				
Uploading to video broadcast e.g. Youtube			✓		

Appendix 3

Incident involving pupils/students	**Teacher to use school behaviour policy to deal with**	**Refer to Head of Department/Head of year/SLT as appropriate**	**Refer to police**	**Refer to technical support staff for action re security/filtering etc**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities**).**		✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓			✓
Unauthorised use of mobile phone/ digital camera/ other handheld device.	✓	✓		
Unauthorised use of social networking/ instant messaging/ personal email	✓	✓		✓
Unauthorised downloading or uploading of files		✓		✓
Allowing others to access school network by sharing username and passwords		✓		✓
Attempting to access or accessing the school network, using another pupil's/student's account		✓		✓
Attempting to access or accessing the school network, using the account of a member of staff		✓		✓
Corrupting or destroying the data of other users		✓		✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓		✓
Continued infringements of the above, following previous warnings or sanctions		✓	Community Police Officer referral	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓		✓
Using proxy sites or other means to subvert the school's filtering system		✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓		✓

The guidance in this policy should be implemented with cross reference to the School's Child Protection, Anti-Bullying and Behaviour Policies.

Appendix 4

Incidents involving members of staff	**Refer to the Head teacher and or Designated Teacher** ***See below**	**Refer to technical support staff for action re filtering, security etc**	**Referral to Bury LADO** **Potential Disciplinary Action**

Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities).	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓		✓
Excessive or inappropriate personal use of the internet/social networking sites/ instant messaging/ personal email	✓	✓	✓
Unauthorised downloading or uploading of files	✓	✓	✓
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	✓	✓	✓
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓		✓
Deliberate actions to breach data protection or network security rules	✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓
Using personal email/ social networking/ instant messaging/ text messaging to carrying out digital communications with current pupils/students or former pupils/students under the age of 18	✓	✓	✓
Actions which could compromise the staff member's professional standing	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓		✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓
Breaching copyright or licensing regulations	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓		✓

***In event of breaches of policy by the Head teacher, refer to the Chair of Governors.**

Internet Permission Form

As part of the school's ICT programme we offer pupils supervised access to the Internet. Before being allowed to use the Internet, all pupils must obtain parental permission and both must sign and return the permission form as evidence of their approval and acceptance of the school rules on this matter.

To protect pupils the school makes use of filtering software which is set to deny access to websites that would undermine the Catholic ethos of the school. However, the steps that we have taken are not intended to replace the responsibility of the individual, and each pupil/student will be held responsible for the correct and proper use of this facility.

Pupil

As a school user of the Internet, I agree to comply with the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by the school.

Pupil's Signature_____ **Date**_____

Parent

As the parent or legal guardian of the pupil named above, I grant permission for them to use electronic mail and the Internet.

I also understand that while the school has taken all reasonable action to deny access to undesirable websites, the responsibility for proper use lies with the individual and pupils will be held accountable for their own actions.

Parent's/carer's Signature_____ **Date**_____

Appendix 6

ST MONICA'S R.C. SCHOOL

ACCEPTABLE USE POLICY

September 2016

St. Monica's is a Catholic community working in partnership with families, schools and parishes to teach the Catholic faith as a way of life. We provide a caring, supportive environment where everyone is of equal worth. Jesus Christ is central to our school and our main aim is that everyone can develop their God given talents and gifts to the full, while growing in faith through prayer and service.

INTRODUCTION

This policy has been drawn up to help staff continue to discharge their duties in a professional manner and to safeguard staff against complaints under current legislation and regulations including the Computer Misuse Act 1990, the Freedom of Information Act 2000, Data Protection Acts 1998 and Human Rights Act 1998 (Appendix A).

Please read the policy carefully. Some of the key points to note include:-

- If your PC is behaving oddly report it to the Technicians without delay
- Keep personal emails to a minimum
- Do not have any expectations of privacy
- Do not use the school internet to access social networking sites
- Do not upload or download copyrighted materials or use “peer to peer” networking even in your own time
- Do not use your school email address as a contact for commercial websites such as Ebay
- The content of emails may be disclosed under the Freedom of Information Act 2000 therefore emails need to be appropriately worded and not be liable to be construed as personally insulting, biased, racist or discriminating. They must not involve an exchange of views about the personality of a third party.
- You must not divulge your password to anyone and log out or lock your computer if it is to be left unattended.
- All outgoing emails will have a legal disclaimer attached.
- Private telephone calls to be kept to a minimum and as far as possible own mobile phones to be used – (see below.)

- Mobile phones – where possible staff should leave their mobile phones in their staff room locker. If taken into a classroom they must not be used under any circumstances and must be switched off and kept out of sight.

Under no circumstances should staff make personal use of the internet during lesson time when teaching, covering absent colleagues or engaged in support work. The internet may only be used in connection with the topic/subject being taught at such times. Personal use should be limited to the times and provisions specified in the Acceptable Use Policy.

The provisions of this document apply to all employees in the execution of their duties, whether on St Monica's R.C. High School premises or at any other location (e.g. at the employee's home).

Specific Responsibilities

All employees are responsible for the confidentiality, security and accuracy of information and information systems during the day-to-day use of the school's ICT facilities, whether working at school or at another site, including an employee's home. Failure to comply with the provisions of this policy or related documents may lead to disciplinary action and/or criminal proceedings.

Reporting "security incidents"

If at any time you suspect that your PC is behaving oddly and so may have been infected with a computer virus or other malicious software, **you must immediately contact the IT Technicians to report the potential security incident.**

Internet

Misuse

You must not knowingly use the School's Internet facilities to access or download the following types of information:

- criminal information (e.g. racist or terrorist propaganda)
- pornography, abusive, defamatory, offensive, obscene, or malicious information

- information that makes improper or discriminatory reference to a person's race, colour, religion or belief, gender, sexuality, age, creed, national origin, disability, caring responsibilities or physique
- any information that might be perceived as damaging or likely to damage the School's reputation

If you need access to any filtered sites in order to do your job, you must ask your HOD to submit a request on your behalf to the ICT Technicians. If you encounter inappropriate information by accident you must inform the ICT Technicians, who will inform SLT as appropriate. The ICT Technical Support team must also ensure that the site is added to the School's Internet Firewall to prevent further access. You must adhere to relevant legislation with regard to your use of the Internet. You must not use the school's Internet facilities to upload, download or otherwise transmit commercial software or any copyrighted materials. You must not use the Internet at any time for either private commercial purposes or personal gain. You must not post advertisements for the sale of goods on Internet Websites (e.g. the 'EBay Internet web site) using your School Email address as your contact details. You **must not** download files for personal use (including video, music, other multimedia, etc.) using "peer to peer networking" or similar technologies even during your own time. This type of traffic can seriously disrupt the performance of the Internet link and interfere with legitimate School business. You **must not** use "instant messaging" software (Microsoft Messenger, Skype, etc.,) on the School's Internet connection, as this contravenes anti-virus controls.

Any employee, agent or contractor found to be in breach or in any way contravening the provisions of this document will be subject to disciplinary action.

Software downloads

You **must not** download software from the Internet for non work-related purposes.

Purchases over the Internet

You can make purchases over the Internet on behalf of the School as long as your Bursar has approved this for your department.

You may make personal purchases on the Internet **in your own time**, at your own expense and entirely at your own risk, providing that the goods are not delivered to School premises.

Email

Personal use

You are allowed to send personal emails **in your own time**, as long as you abide by the provisions listed in Section 'Misuse'. **You should have no expectation of privacy for any personal email that you send or receive via your work email account.**

Use and Misuse

You must be aware that you and/or the School might be held liable in law for any email sent by you that could be construed as libellous or defamatory. It is your responsibility to ensure that your emails cannot be construed in this way. If you are unsure of the suitability of the content of an email, you should seek clarification from your line manager.

Certain types of misuse of the email system could lead to disciplinary action under the School's existing policies e.g. The Race Relations Amendment Act, the Equal Opportunities and the Harassment at Work policies.,

You **must** comply with the provisions listed below in your use of the School's email system; failure to do so may lead to disciplinary action.

1. You must not exchange frivolous personal emails with other School employees.

2. Any email contact with pupils/students must be done through the school email system and must be appropriate. Staff must not contact pupils/students or former pupils/students under the age of 18 using personal email accounts.

3. You must keep personal emails to a minimum using a non work email account.

4. You must not use the School's email system in pursuit of any private commercial interests or for personal gain.

5. You must not send unsolicited advertising or promotional material not connected with the School's business on the School's email system

6. You must not use the School's email system for fraudulent purposes or in connection with a criminal offence or unlawful activity;

7. The sending of email messages which are abusive, defamatory, offensive, obscene, or malicious; or which make improper or discriminatory reference to a person's race, colour, religion or belief, gender, gender reassignment, sexuality, age, creed, national origin, disability, caring responsibilities or physique; or which might be perceived as damaging or likely to damage the School's reputation are prohibited.

8. If you receive an email that falls within any of the above mentioned categories, you must report it to the SLT.

9. You must not send emails to cause annoyance, inconvenience or needless anxiety

10. It is forbidden to make emails appear as though they have originated from someone else.

11. You must not post advertisements for the sale of goods on Internet Websites (e.g. the 'E-Bay Internet website) using your Bury School Email address as your contact details.

12. You must not access emails whilst your computer is actively linked to a whiteboard or projector.

Monitoring email use

Email system is subject to regular monitoring and filtering for security and / or network management reasons. We reserve the right to intercept emails that contravene the provisions of this policy. You should have no expectation of privacy for any personal email that you send or receive via your work email account.

SLT Managers may access an employee's email account without the employee's permission in exceptional circumstances and only with the explicit written authorisation of the Headteacher or Chair of Governors in the Headteacher's absence, such as:

1. Absence (e.g. due to sickness, or business commitment) where there is a need to access messages in order to carry out the normal functions of the School.

2. Where there is a suspicion of misuse.

Legal Implications

In particular, it should be noted that the contents of emails may be disclosed under the Freedom of Information Act 2000. Refer to Appendix A for further details of this Act. With this in mind, you must word emails appropriately in all cases and, in particular, not send emails that contain references which could be construed as:

- Personally insulting to a third party
- A show of personal bias by an employee against someone / organisation
- Exchange of views about the personality of a third party

Emails and Harassment / Pornography

It is not permitted to transmit, retrieve or store information that is offensive, discriminatory, harassing, or pornographic, on any of the computer systems or magnetic media belonging to the School. If you receive an email of this nature, you must inform SLT.

Emails and confidential information

You must not assume that electronic communications are totally private; emails may be intercepted or misdirected. Email messages cannot be protected from unauthorised access caused by the user failing to maintain password confidentiality or leaving the computer unattended when logged onto the system. It is your responsibility to not divulge your password to anyone and to ensure you log out of, or lock, your workstation when it is left unattended. You should not expect any messages sent on the School's network between the sender and the recipient(s) to be for private viewing only. This should be taken into consideration should you need to send confidential, personal or other sensitive information via email. When sending confidential or sensitive information by email, the measures below must be followed:

- Do not send e-mails and attachments containing sensitive information to a generic email address (e.g. Info@companyname.org) the email address should be a named individual.
- Make sure that you have sent data to the right person and check that they have received it
- It is possible to increase the security of information sent by email by placing it in a 'zip' file and password-protecting the zip file. Even if you are sending e-mail and attachments internally, remember it may not be *read* in a secure environment as School employees can remotely access their e-mails.

School Telephones

Private telephone calls – the school telephones may be used in an emergency only.

Private telephone calls should be made in your own time, where possible, using own mobile phone. However, mobile phones should not be used in the classroom.

International calls may be made provided they are regarding school business.

Any malicious telephone call received must be reported to a member of the SLT.

SMS Testing Service is another mode of communication that enables users to send texts to mobile phones and landlines. This service must not be used in any way that conflicts with e-mail or telephone acceptable usage.

SEPTEMBER 2016

Appendix A - The Legal position

Everyone is obliged to abide by relevant UK and EC Legislation/guidance / directives / regulations and this and any other relevant policy of this Authority in connection with the use of ICT. An illustrative list of relevant legislation / guidance / directives / regulations is set out below:

- Copyright, Designs and Patents Act 1988
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Thefts Act 1968 and 1978
- Human Rights Act 1998
- Regulation of Investigatory Powers (RIP) Act 2000
- Police and Criminal Evidence Act 1984 [PACE]
- Caldicott Report Principles
- Data Protection Acts 1998 (See Section 6.4)
- Fraud Act 2006

The following may also be relevant to aspects of the operation or acquisition of information systems:

- Copyright, Designs and Patents Act 1988
- Freedom of Information Act 2000
- Trademarks Act 1994
- Computer Misuse Act 1990
- Human Rights Act 1998
- Regulation of Investigatory Powers (RIP) Act 2000
- Police and Criminal Evidence Act 1984 [PACE]
- Caldicott Report Principles
- Data Protection Acts 1998 (See Section 6.5)

The legislation/guidance/directives/regulations etc. listed in this policy is not exhaustive in relation to information security but is intended only as indication of the range of measures that must be addressed / complied with. It is no substitute for reading and/or taking legal advice on the actual legislation Any reference to any statute/ directive/guidance/regulation includes any statutory modification or re-enactment thereof.

Copyright, Designs and Patents Act 1988

Software is subject to the same copyright laws as other intellectual property. Only software licensed from a software company, or developed by the Council's staff or agents, shall be installed and used. Public Domain or Shareware software is available licence-free, or on a 'try before you buy' basis. Such software must only be used with the express permission of Management and should be registered and/or licence fees paid. Any form of software media can be a source for viruses. Accordingly, all media must be virus checked before use.

Copying of licensed software must only be in accordance with the licence. The copyright of software developed by Council staff, or its agents, is vested in the Council.

You must not copy, for your own use or gain, software licensed to the Council.

Computer Misuse Act 1990

This Act creates a criminal offence where there is:

Unauthorised access to computer 'material'

Unauthorised access with the intent to commit or facilitate a further, more serious, offence

Unauthorised modification of any computer 'material'

Freedom of Information Act 2000

The Freedom of Information Act 2000 (FOIA 2000) makes provision for the disclosure of information held by public authorities or by persons providing services for them. A request for information is any request which is in writing (including email or fax), in legible form and states the name and address of the correspondent.

The Authority must comply with the request for information promptly and, in any event, not later than 20 working days. The Act describes what information is exempt from the requirement to give information, and they can be either ‘Absolute’ or ‘Qualified’. Where a qualified exemption applies, the Authority will have to apply a ‘Public Interest Test’. Each Council department has a Document Management and Retention policy for all electronic and paper records, which must be adhered to. Keeping records for longer than is necessary breaks the 5th Data Protection Principle. In addition, the contents of emails may be disclosed under this Act; therefore all emails should be appropriately worded in all cases.

Theft Acts 1968 and 1978

It is a criminal offence to appropriate any other person's property dishonestly with the intention of permanently depriving that person of it. This includes intellectual property, and IT hardware, software and any related equipment, installation or facility. It is also a criminal offence to obtain services or evade any liability

Human Rights Act 1998

The Act brings into our law various human rights, including in particular, the right to respect for a person's private and family life which includes the right to private communications. The right can be interfered with in certain situations. In particular the monitoring by an employer of personal e-mails sent by an employee at work can be justified on the basis that:-

1. The interference is in accordance with the law (see Regulations below)

2. It is necessary to protect the rights and freedoms of others, or to prevent crime and disorder

3. The interference is proportionate i.e. the rights of the person whose e-mail is being intercepted are balanced against the rights of the employer and it is not excessive. So if it is within the law (see below) and it prevents the sending of offensive or libellous emails, for example, it is justified because it prevents harassment of other employees or members of the public, and prevents damage to the Council's reputation as a public authority and thus the public of Bury.

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

(made under the Regulation of Investigatory Powers Act (RIPA) 2000.

These Regulations set out a new legal framework to govern the interception of communications, and establishes when it is lawful to do so. Organisations may authorise to monitor or record communications systems without consent for the following purposes:

1. in order to establish the existence of facts relevant to the employer's business

2. to ensure compliance with regulatory practices or procedures

3. to ensure that standards are being achieved (e.g. in call centres)

4. in the interests of national security

5. to prevent or detect crime

6. to investigate unauthorised use of a system

7. to secure the effective operation of the system (e.g. to check for viruses)

8. to check whether the communications are relevant to the business (e.g. where the employee is absent and the employer needs to check the employee's emails)

9. to monitor communications made to anonymous telephone lines In order to make such interceptions without consent, the employer must make all reasonable efforts to inform its staff that communications may be intercepted.

Caldicott Report Principles

1. Justify the purpose for which information is required;

2. Don’t use person-identifiable information unless it is absolutely necessary;

3. Use the minimum necessary person-identifiable information to satisfy the purpose;

4. Access to person-identifiable information should be on a strict need-to-know basis;

5. Everyone with access person-identifiable information should be aware of their responsibilities;

6. Understand and comply with the law.

Computer Evidence in Criminal Cases

It is now not necessary to prove the reliability of a computer before any statement in a document produced by a computer can be admitted in evidence. However, if it is shown that the computer is not working properly, it will affect the weight given to the evidence by the court. Therefore, this necessitates the requirement for maintenance to be undertaken periodically.

The following may also be relevant to aspects of the operation or acquisition of Information systems:

- Children Act 1989
- Companies Act 1985
- Criminal Justice and Public Order Act 1994
- Defamation Act 1996
- European Directives and Regulations
- Human Rights Act 1998
- The Health and Safety (Display Screen Equipment) Regulations 1992
- Local Government Finance Act 1982
- Race Relations Act 1976
- Sex Discrimination Act 1975
- The Theft Act 1968
- Transfer of Undertakings (Protection of Employment) Regulations 1981
- RIP Act 2000

N.B. - This second list is only intended to be indicative of the range of issues that must be considered. It is not a comprehensive list of legislation relating to information security.

Fraud Act 2006

Under the Fraud Act 2006, it is a criminal offence to:

- dishonestly makes a false representation intending to make a gain for himself or cause loss to another; or
- dishonestly fails to disclose information being under a legal duty to do so intending to make a gain for themselves or cause loss to another; or
- dishonestly abuses their position where they occupy a position in which they are expected to safeguard the interests of others or expected not to act against the financial interests of others

This section of the policy deals with data and hardware issues.

Sections of the policy most relevant to line managers and teaching staff are highlighted.

Computer Systems and Data

Anti-Virus Software

Anti-virus software must be installed on all file-servers, and networked and standalone PCs. The IT technicians are responsible for ensuring that the anti-virus software is automatically updated on all file-servers and networked PCs.

Line managers are responsible for ensuring that all standalone PCs in their department are regularly updated with the latest Anti-Virus software. The Anti- Virus software updates are supplied by the IT technicians on request.

Procedures for Virus Controls

The following procedures must be followed to minimise the risk of software virus infection:

- The IT technicians must be contacted about software installations.

- You must not open files attached to unsolicited Emails that do not originate from known or reputable sources. If in doubt, contact the IT technicians.

- All School-owned laptops must be connected to the School network when notified to receive the latest anti-virus software and security software updates.

Systems Development

All computer programmes and data developed by the School are for the sole purpose of the School's business and access by employees is solely for this purpose except by express written permission of the Headteacher.

The School owns the Copyright for all Software that has been developed by Employees and Contractors in the course of their employment with the School, for specific use by the School.

Control of proprietary software copying

Proprietary software products are usually supplied under a licence agreement that limits

the use of the products, and limits the copying to back-up copies only.

In line with the Copyright, Design and Patents Act 1988, it is School policy that no copyright material is to be copied without the owner's consent.

If copies of software in excess of those specified in the licence agreement are required the owner's written consent must be obtained. This consent must then be held together with the licence.

Data Security

All School data remains the property of the School and is confidential. All employees must take due care when handling and sharing School data to prevent unauthorised access to information; this applies to all information, whether it's held on a computer or on any other media, including paper.

Line Managers' responsibilities

Line Managers are responsible for agreeing and monitoring procedures for ensuring the security of work, information, data and files under an employee's control. Where individuals need to work from home or out of the office, you may consider the option of Remote Access to ICT Systems, which provides secure access to ICT systems and files. Contact the IT technicians to arrange this.

Managers must take due care in the positioning of PC monitors in public areas, taking into consideration the sensitivity of the information that may be displayed on them.

Users' responsibilities

Whether working at school or at another site, including the employees' home, employees must take all reasonable precautions to protect information relating to employment with the School.

Computer files not held on the School's networked drives must be regularly backed up onto disc and stored securely. Special care must be taken to safeguard the security of School data stored on removable media, in particular CDs, DVDs, Pen Drives, Digital Camera memory cards, Digital Pens, and data held on PDAs and Smartphones.

It is recommended that employees with remote access rights keep work life and domestic life separate. In particular, where there is a risk that other household occupants might gain access to work related computer files, these should be password protected.

Care should be taken not to inadvertently disclose passwords.

Employees with remote access rights should comply with the School's systems and departmental procedures for keeping anti-virus software up-to-date and logging off or locking their workstation when a computer is not in use.

Disposal of waste computer printed output **must** be done with due regard to its sensitivity. The Headteacher is responsible for deciding on retention periods of printouts and ensuring that all legal requirements are met. After the expiry date confidential waste **must** be shredded prior to disposal.

If you are disposing of pen drives, CDs, DVDs and any other electronic devices, do so securely, so that the information previously stored on them cannot be recovered.

CDs and DVDs can be scratched to damage them and therefore make the data unreadable. If you need to dispose of a pen drive, please contact the IT technicians.

Do not place any of these portable devices in the rubbish bin.

Sending personal data on paper or on portable media

If it is necessary to send personal data to another organisation on disk or other portable media such as CD, DVD, memory stick, the following measures must be followed:

- Consider what the effect would be on individuals if the data were lost

- Use Royal Mail special delivery or a courier firm that has track and trace

Computer and Network Management

General

It is vital that backup procedures are in place and documented to maintain the availability, integrity and confidentiality of data.

The IT technicians must ensure that appropriate back-ups are undertaken for the System and all fileservers located in the server room.

HODs are responsible for ensuring that appropriate back-ups are undertaken for all standalone PCs and laptops located in their department.

Procedures

The following procedures must be followed:

- Media containing back-ups must be stored in a lockable cupboard.
- The latest back-up hard drive should be stored away from the primary site.
- Recovery procedures using back-ups are tested on a weekly basis as pupil/student work is restored after deletion.

Fileservers

The SLT and IT technicians must together decide on appropriate back-up procedures for fileservers. Where fileservers are located in user departments, a nominated user is responsible for the loading and storing of back-up drives. All back-up hard drives must be clearly marked and stored in a secure location.

The Email System

The cloud based email system (Office365) is backed up every day by Microsoft and is held for 6 months in case retrieval is required.

Users are responsible for the management of their own email account and users can restore items they have deleted from their deleted items through an automated recovery process available on via mail.office365.com

PCs, Laptops, Tablet PCs, PDAs and all mobile devices

All users whose PCs have access to a fileserver must store all school related data on the fileserver and not just on the local hard drive of the PC.

Users who do not have access to a fileserver must make appropriate arrangements to ensure all data is regularly and safely backed-up. You should contact the IT technicians if you are unsure of the best back-up solution for your data.

Whilst working in PC applications, you should regularly save your work to avoid losing data in the case of a system failure.

If you are using a laptop off the network, you must ensure that the data is backed up regularly to CDs, DVDs or pen drives, which should be stored securely.

This data must also be transferred to a fileserver, where possible.

Data Storage

Back-up copies of data must be held in a safe and secure environment separate from the computer installation. The selection of this secure area should take into account the same hazards as the computer installation itself. The location should be sufficiently remote from the computer installation to avoid the possibility of any disaster affecting the computer also affecting the back-up.

Recovery from Back-up

It is important to check regularly that the recovery from back-up files works satisfactorily. This **must** include being able to identify and re-input all important data that have been entered since the last back-up was taken.

Network Management

Access

If you require access to the School network you must contact your line manager.

When an employee leaves the School, their access to computer systems and data **must** be deleted on the employee's last working day. It is the responsibility of the line manager to request this deletion via the IT technicians.

Similarly, line managers must inform the IT technicians when any staff change jobs within the School to amend that user's systems access, as appropriate.

Administrator Access

The privilege levels assigned to members of staff must be commensurate with the tasks they are expected to perform.

External connections to the network

The use of modems on PCs connected to the School's network can seriously compromise the security of the whole of the School network. You **MUST** obtain specific approval from the Headteacher for the use of a modem on any networked computer.

The unapproved use of a modem will be considered a breach of the School's Security Policy.

Where PCs use remote access to the School's network, the session must be closed down should a PC be left unattended for any amount of time.

Suppliers' and External agencies' access to the School Network

No partner agency or 3rd party supplier should be given details of how to access the School's network without the formal approval of the Headteacher.

The disclosure of connectivity details without the formal approval of the Headteacher will be considered a breach of the School's Security Policy

General

You must not intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network.

Fault logging

You should report all apparent faults with computer services to the IT technicians, who will deal with the matter as soon as possible.

Change Control

When implementing any change to IT equipment or software used in the provision of any agreed service, the IT technicians will maintain and follow change control procedures to ensure minimal disruption to service.

The IT technicians will ensure that:

- changes are tested within a test environment, when possible, and implemented using change control procedures;

- compatibility is maintained between the changed item and all related hardware and software (whether operating system or application software);

- Changes are scheduled in order to minimise risk to the operation of services.

Where a major system change is required on a system, the SLT and IT technicians will agree an implementation date in advance, after first assessing any impact on other related services.

The IT technicians must ensure that advice is provided to departments to ensure that no requested change compromises security, ICT standards, ICT Strategies, other relevant codes, policies or standards, or conflicts with other user demands.

Where the IT technicians wishes to implement a change that requires a period of downtime for any service, or alters the usage of the service, the IT technicians will notify the system's key users in advance. These key users must then notify all other users of that system within their year group or department.

Physical Security

Server Room

Environmental Control

The Server Room must have environmental controls to maintain humidity and temperature.

Emergency 'power off' facilities must be available in the Server Room.

UPS (Uninterrupted Power Supply) must be in place to avoid failure following lightening or power surges.

Physical Access control

The Server Room doors must be secured at all times, and access restricted to authorised personnel only.

A log must be kept of all visitors, maintenance and engineering staff given access to the Server Room .

All visitors to the Server Room must have visitor badges.

Employees must bring to the attention of their line manager any unauthorised access to

the Server Room .

All known breaches of security in the Server Room must be reported to the IT technicians, who will inform the relevant SLT staff.

Such incidents include:

- Emergencies and disasters such as flood, fire, power failure and theft.

- Any suspected security violations

- Any suspected sabotage attempts

- Computer virus contamination

IT Equipment located in Departments

All fileservers located outside of the Server Room must be sited in a physically secure environment.

The user department must ensure that doors and windows are properly secured.

The user department must not allow such equipment to be moved, modified, maintained or repaired by any person other than those authorised or approved by the IT technicians.

All Fileservers and communications equipment must remain switched on. Such equipment should be properly identified and marked.

Access codes to the School's buildings must not be disclosed to unauthorised personnel.

Equipment Security

Equipment should be sited:

- to avoid unauthorised access or theft; workstations handling sensitive data should be positioned so as to eliminate the risk of overlooking.

- to reduce risks from environmental hazards, for example, heat, fire, smoke, water, dust, vibration, chemical effects, electrical supply interference and electromagnetic radiation.

Other considerations:

- Equipment should not be located near windows, where possible

- Appropriate safety equipment should be installed, such as heat and smoke detectors, fire alarms, fire extinguishing equipment and escape routes. Safety equipment should be checked regularly, in accordance with manufacturers' instructions and Health & Safety procedures.

Personal use of the School's IT equipment

IT equipment is provided primarily for business-related tasks only, but with the prior agreement of your line manager, you may be permitted to use the equipment in your own time for personal use. You may be required to contribute to the cost of computer consumables in respect of personal use.

However, you must **not** use the school file servers to store personal files e.g. photographs, music and movie files. Storing these files takes up valuable School resources and can seriously hamper the recovery of School data in a disaster recovery situation.

Laptop Computers / PDAs / Mobile Phones / Home Workers

All staff have a responsibility to ensure the laptop loaned to them is used appropriately.

When taking IT equipment off-site, you should ensure it is insured under the School's All Risks policy.

The provisions of this Policy apply to the use of IT equipment used off School premises, and users must be made aware of their responsibilities when taking IT equipment off-site.

If any inappropriate material is found on Laptops, PDAs, or Tablet PCs, the Head Teacher must be informed immediately. The School reserves the right to inspect and recall IT Equipment at any time.

Users' responsibilities

Adequate steps must be taken to ensure the physical safety of IT equipment and the safety of any data stored on it. This applies to laptops, tablet PCs, PDAs, and any removable media, including Pen Drives, CDs, DVDs, Digital Camera Memory Cards, Digital Pens etc.

School laptop computers and similar devices must not be taken outside of the United Kingdom without the Headteacher's permission.

Advice on the use of pen drives, CDs, DVDs and other portable devices

- **Do not** store confidential/sensitive information on these devices (unless encrypted and protected with a secure password).

- **Do** delete confidential/sensitive information from (encrypted) devices as soon as it no longer needs to be there.

- **You are personally responsible for the safety of any School information/data you store on such devices**. If you remove it from School premises you are responsible for ensuring its safe transport.

- If you lose a device, report the loss to your line manager and/or the owner of the data immediately.

- Pen drives are not a reliable long term storage medium

System Security

Access control

Each user should be allocated access rights and permissions to computer systems and data commensurate with the tasks they are expected to perform.

User registration

If you require access to the School's computer systems, you must contact your line-manager.

Systems Access Management

When an employee leaves the School, their access to computer systems and data **must** be deleted on the employee's last working day. It is the responsibility of the Line Manager to request this deletion by the IT technicians.

Similarly, Line Managers must inform the IT technicians when any staff change jobs within the School and submit a request to the IT technicians to amend that user's systems access, as appropriate.

User password management

Access to the School's computer network must be dependent upon the entry of a valid User id and Password.

Each user **must** have their own User id and password.

All users must have unique passwords for both connecting to the network and for access into different systems.

The password system must 'end session' after three unsuccessful log-in attempts.

Where PC systems or files are to be password protected, departments must ensure that suitable procedures are in place to control password use.

User Responsibilities

Employees must not examine, change or use another person's email account, files, or output for which they do not have explicit authorisation.

Password use

Passwords should be six characters long, should not be readily "guessed" i.e. not in a dictionary and comprise a mixture of alphabetic and numeric characters, with at least two capitals and two numbers.

Avoid the use of passwords based on dates, family names, car registration numbers, telephone numbers, user names, or other easily guessed words.

Passwords **must never** be disclosed to anyone.

Keep your password secure and private.

The use of another person's User id and Password is not allowed.

Temporary passwords **must** be changed at the first log-on.

Passwords should not be written down.

Passwords **must** be changed immediately if it is suspected that it has been compromised, and the matter reported to the IT technicians.

Passwords **must not** be included in any automated log-on procedures, macros or function keys.

Unattended user equipment

PCs must not be left unattended when logged-in to applications. Whenever you leave your PC you **must** lock the screen to prevent anyone using it in your absence. This is to protect School data and the integrity of your own email facilities.

You must log out of systems and the network every night and switch off your PC, unless specifically requested not to do so.

In addition to security considerations, this saves electricity and reduces the risk of fire.