Baytree School

E Safety Policy
March 2018

Introduction

This document is a statement of the aims, principles, strategies and procedures for E-Safety throughout the school.
E-Safety is essentially safeguarding children and young people in the digital world. It is about learning to understand and use technologies in a positive way, and about supporting children and young people to develop safe online behaviours (both in and out of school).
E-Safety encompasses not only interest technologies, but also other means of electronic communications, such as mobile phones, games consoles and wireless gadgets. There has been an increasing convergence of technologies over recent years, for example, MP3 players and electronic readers that can access the internet, and mobile phones and hand held devices that can take photos, play games, access the internet and play music.
The Internet is an essential element in 21st century life for education, business and social interaction. This school has a duty to provide students with quality Internet access as part of their learning experience. The Internet is part of the statutory curriculum and an entitlement for pupils as part of their learning experience. It is used in this school to raise educational standards, promote pupil achievement and as a necessary tool for staff to support their professional work. The Internet also enhances the school's management information and business administration systems.
However, in common with other media such as magazines, books and videos, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor North Somerset Council can accept liability for the material accessed, or any consequences of Internet access.

The Benefits to the School
Benefits of using the Internet in education include:
· A vast range of free and subscription educational resources to enhance the learning experience of pupils.
· Access to world-wide educational resources including museums and art galleries;
· Educational and cultural exchanges between pupils world-wide;
· Access to experts in many fields for pupils and staff;
· Staff professional development through access to national developments, educational materials and good curriculum practice;
· Communication with support services, professional associations and colleagues;
· Exchange of curriculum and administration data with the LA and DfE.
· Mentoring of pupils and provision of support for them and teachers.

Internet Access
Internet access will enhance learning, pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
· School Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the pupils.
· Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
· Internet access will be planned to enrich and extend learning activities.
· Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
· Parents and pupils are required to return a signed copy of the pupil "Acceptable Use Policy" at each Key Stage (see appendix 1).
· All staff, visitors and volunteers must read and sign the staff "Acceptable Use Policy" before using any school ICT resources (see appendix 2).
All visitors/volunteers must read and sign the visitors "Acceptable Use Policy" before using any school ICT resources (see appendix 6)

Management of E-mail
· Staff and pupils may only use approved e-mail accounts on the school system Office 365. This is administered by Issy Johnson where new accounts can be set up or old ones deleted. There are still some North Somerset email accounts still accessible.
· Pupils must have adult supervision whilst using E-mail.
· Pupils must immediately tell a teacher if they receive offensive e-mail.
· Pupils must not reveal personal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone without specific permission.
· E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
· The forwarding of chain letters is not permitted.

Internet content.
· Pupils will be taught to question information before accepting it as true.
· The school will ensure that use of Internet derived materials by staff and pupils complies with copyright law.
· Pupils will be made aware that the writer of an E-mail or the author of a Web page may not be the person claimed.
· Pupils will be encouraged to tell a member of staff immediately if they encounter any material that makes them feel uncomfortable.

The School Website
· The point of contact on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
· Website photographs that include pupils will be selected carefully and will not enable individual pupils to be identified. Photographs will only be published with parental permission (see appendix 2).
· Pupils' full names will not be used anywhere on the Website, particularly in association

with photographs.
· The Headteacher will delegate editorial responsibility to the Bursar to ensure that content is accurate and quality of presentation is maintained.

Internet Dangers and Risk Assessment
Baytree School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
An E-safety co-ordinator has been appointed to oversee Internet dangers, risk assessment and matters arising from Internet use. However neither the school nor North Somerset Council can accept liability for the material accessed, or any consequences of Internet access.
· Staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
· The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Social networking and personal publishing
· The school via South West Grid for Learning (SWGfL) will block access to social networking sites.
· Newsgroups will be blocked unless a specific use is approved.
· Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
· Pupils will be advised never to give out personal details of any kind which may identify them or their location or to place personal photos online or to arrange to meet someone without specific permission from parents/carers

Cyberbullying
'Cyberbullying can be defined as the use of Information Technology (IT), particularly mobile phones and the Internet, deliberately to upset someone else.'
It is not a specific criminal offence but there are laws that apply to associated behaviour, such as the Protection from Harassment Act 1997 or the Malicious Communications Act 1988. It is important that children and young people keep any evidence of cyberbullying and that they realise that the police will be able to trace the originator of any messages.

Many young people and adults find using the internet and mobile phones a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the internet, they can often feel very alone and, a once previously safe and enjoyable environment or activity, can become threatening, harmful and a source of anxiety.
Cyberbullying (along with all forms of bullying) will not be tolerated in school. All incidents reported will be recorded and investigated.

Filtering
· The school will work in partnership with the LA, DfE and the Internet Service Provider (South West Grid for Learning SWGfL)to ensure systems to protect pupils are reviewed and improved.

· If staff or pupils discover an unsuitable site, the URL (address) and content must be reported to the Bursar and the Internet Service Provider informed in order for the site to be blocked.

Emerging technologies

· Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school is allowed.
· Mobile phones must not be bought into school unless the Headteacher has given permission. The sending of abusive or inappropriate text messages is forbidden.
· The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
· The E-safety co-ordinator will ensure that the E-safety policy is implemented and compliance with the policy monitored (all staff will be required to sign a form declaring they have understood the E-Safety Policy and it's procedures)

Information system security

· School ICT systems capacity and security will be reviewed regularly by 2IT Systems who regularly monitor the network
· Virus protection will be updated regularly (Sophos purchased annually)
· Security strategies will be discussed with North Somerset Council and the IT Company who support the curriculum
· Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

The Policy and Pupils

The E-Safety policy will be introduced to the pupils through lessons and constant reinforcement.
· E-safety rules will be posted in all rooms where computers are used and discussed with pupils at the start of each year (see appendices 3 and 4). Implementation of the E-safety rules will be checked regularly by the E-safety co-ordinator.
· Pupils will be informed that Internet use will be monitored and access will be withdrawn if the facility is abused (see appendix 5 regarding sanctions).
· The school will keep a record of all pupils who are granted Internet access. The record will be kept up-to-date, for instance if a pupil's access is withdrawn or if pupils leave or join the school (see appendix 5).
· Pupils will be informed that network and Internet use will be monitored.
· Instruction in responsible and safe use will precede Internet access.
· Pupils' work can only be published on the website with the permission of the pupil and parents.

The Policy and Staff

It is important that all staff are confident using the Internet in their work. The School Internet Policy will only be effective if all staff subscribe to its values and methods.
· All staff must read and sign the 'Acceptable Use Agreement' before using any school ICT resource.
· The school will keep a record of all staff who are granted Internet access. The record will be kept up-to-date, for instance if a member of staff leaves.
· All staff including teachers, supply staff, teaching assistants and support staff, will be

provided with the E-safety Policy, and its importance explained.
· Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
· Staff development in safe and responsible Internet use will be provided as required.
· Any breaches of the Staff Acceptable Use Policy will be referred directly to the Headteacher.
· Staff should be aware that if using social networking sites their profiles should be private and that the school should not be discussed. It is also not acceptable to have pupils (or past pupils) as online contacts. It is suggested that Parents/Carers are not on-line contacts

ICT Security
The school ICT systems will be reviewed regularly with regard to security.
· Virus protection will be installed and updated regularly by 2IT Ltd (IT Support)
· Security strategies will be discussed with the LA/SWGfL
· Photographs of pupils must only be taken using school equipment, in exceptional circumstances with specific authorisation personal cameras can be used and images immediately transferred to school network and then deleted from camera memory. All images must be stored in the staff area on the network not on curriculum computers or teachers laptops only if on equipment that has encryption software for reports/pupil evidence
· Administrative data sent over the Internet will be encrypted or otherwise secured.
· Use of portable media such as floppy disks, memory sticks and CD-ROMs will be reviewed. Portable media may not be brought into school without specific permission and a virus check.
· Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to E-mail.
· Files held on the school's network will be regularly checked.
· 2IT manager will ensure that the system has the capacity to take increased traffic caused by Internet use.

Complaints
· Responsibility for handling Internet misuse incidents will be taken by the E-safety co-ordinator.
· Any complaint about staff misuse must be referred to the Headteacher.
· Complaints of a child protection nature must be dealt with in accordance with school child protection procedures which adhere to the North Somerset Safeguarding Children Board
· Pupils and parents will be informed of the complaints procedure.
· Parents and pupils will need to work in partnership with staff to resolve issues.
· There may be occasions when discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.
· Sanctions available for pupil misuse include:
- interview/counselling by E-safety co-ordinator;
- informing parents or carers;
- removal of Internet or computer access for a period of time.

Internet and the community

· Where possible the school will liaise with local organisations to establish a common approach to E-safety.

Parental Support

· Parents' attention will be drawn to the School E-safety policy in newsletters, the school prospectus and on the school website.
· Parents will be asked to sign an Internet approval letter (Appendix 5)
· Internet issues will be handled sensitively to inform parents without undue alarm.
· A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.

Signed Chair of Governors:

Date:

Review Date:

APPENDIX 1

Acceptable User Policy

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and learners 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. Our school's AUP e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a policy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the learners themselves.

South West Grid for Learning Trust, School E-Safety Policy, February 2009

Development/Monitoring of this Policy

The implementation of this e-safety policy will be monitored by the E-safety Co-ordinator, ICT/E-safety Governor along with the SLT.

Monitoring will take place at least once a year.

The Curriculum Development Committee will receive a report on the implementation of this policy generated by the monitoring group at regular intervals.

The E-safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.

Baytree will monitor the impact of the policy through:

- Logs of reported incidents;
- SWGfL monitoring logs of internet activity;
- Surveys/questionnaires of learners, parents and staff.

Roles and Responsibilities

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

Role	Responsibility
Governors	• Approval of the E-Safety policy and for reviewing its effectiveness. • Appoint a member of the Governing Body as E-Safety Governor. The role of the E-Safety Governor will include: • regular meetings with the E-Safety Co-ordinator • regular monitoring of e-safety incident logs • regular monitoring of filtering / change control logs • reporting to relevant Governors committee / meeting
Headteacher and SLT	• The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator • The Headteacher and SLT are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant. • The Headteacher and SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. • The SLT will receive regular monitoring reports from the E-Safety Co-ordinator. • The Headteacher and another member of the SLT will be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
E-Safety Co-ordinator	• Leads the e-safety committee. • Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents. • Ensures that all staff is aware of the procedures that need to be followed in the event of an e-safety incident taking place. • Provides training and advice for staff. • Liaises with the Local Authority. • Liaises with school ICT technical staff. • Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments. • Meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs. • Attends relevant meetings / committee of Governors

	• Reports regularly to SLT.
ICT Technician	The ICT Technician is responsible for ensuring: • That the school's ICT infrastructure is secure and is not open to misuse or malicious attack. • That the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance. • That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed. • SWGfL is informed of issues relating to the filtering applied by the Grid. • That he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant. • That the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator and /Headteacher for investigation, action, sanction. • That monitoring software / systems are implemented and updated as agreed in school policies.
Teaching and Support Staff	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, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP). • They report any suspected misuse or problem to the E-Safety Co-ordinator for investigation / action / sanction. • Digital communications with students / learners should be on a professional level and only carried out using official school systems. • E-safety issues are embedded in all aspects of the curriculum and other school activities. • The school's e-safety and acceptable use policy is shared and understood by learners. • Learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • They monitor ICT activity in lessons, extra curricular and extended school activities. • They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

	• In lessons where internet use is pre-planned, learners 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. • Appropriate security settings are in place for use of social networking sites, so to protect professional identity and the safety of pupils. • School business or dialogue regarding pupils and colleagues is not shared digitally via social networking sites or email.
Child Protection Officer	Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from: • sharing of personal data • access to illegal / inappropriate materials • inappropriate on-line contact with adults / strangers • potential or actual incidents of grooming • cyber-bullying
E-Safety Committee	Members of the E-safety committee (or other relevant group) will assist the E-Safety Coordinator (or other relevant person, as above) with: • The production / review / monitoring of the school e-safety policy / documents. • The production / review / monitoring of the school filtering policy.
Learners	Are responsible for using the school ICT systems in accordance with the appropriate Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so • Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying. • 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 covers their actions out of 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 every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, and website information about national / local e-safety campaigns / literature. Parents and carers will be responsible for: • Endorsing (by signature) the Student / Pupil Acceptable Use Policy • Accessing the school website in accordance with the relevant school Acceptable Use Policy.

Education

A planned e-safety programme, highlighting key e-safety messages, will be provided as part of ICT and PSHE lessons, and should be regularly revisited; this will cover both the use of ICT and new technologies in school and outside school.
Learners should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

Learners should be helped to understand the need for the student / pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school

Students / learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
Rules for use of ICT systems / internet will be posted in all rooms
Staff should act as good role models in their use of ICT, the internet and mobile devices

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

In lessons where internet use is pre-planned, it is best practice that students / learners 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.

Where students / learners are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Learners should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety Coordinator will receive regular updates through attendance at SWGfL / LA / other information / training sessions and by reviewing guidance documents released by BECTA / SWGfL / LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required

Technical

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance.
There will be regular reviews and audits of the safety and security of school ICT systems
Servers, wireless systems and cabling must be securely located and physical access restricted
All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Technician and will be reviewed, at least annually, by the E-Safety Committee.
All users will be provided with a username and password by the ICT Technician who will keep an up to date record of users and their usernames.
The administrator passwords for the school ICT system, used by the ICT Technician must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
Users will be made responsible for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
The school maintains and supports the managed filtering service provided by SWGfL
In the event of the ICT Technician needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.

Any filtering issues should be reported immediately to SWGfL.
Requests from staff for sites to be removed from the filtered list will be considered by the ICT Technician and ICT Subject Leader. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee
School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
Remote management tools can be used by staff to control workstations and view users' activity
Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

APPENDIX 2

Baytree School
ACCEPTABLE USE AGREEMENT FOR THE INTERNET, E-MAIL AND SCHOOL ICT NETWORK & EQUIPMENT

All members of staff and visitors

- Children should only use the Internet supervised, and all weblinks checked prior to the lesson when possible.

- The entire ICT infrastructure (server, computers, network, peripheral hardware, software) is owned by the school and may be used by learners to further their education and by staff to carry out their professional duties.

- Access to the network should only be made through your authorised account using your own username and password. This should be kept secret by yourself and the network administrators.

- The school ICT equipment and network must be treated with due care, and not tampered with. Report any technical problems to the network administrators or ICT technicians via the log book.

- New software must only be run or installed on a school computer and network by the ICT Technician.

- Software from the internet must only be run or installed on a school computer and network by the ICT Technician.

- Staff may load or download software on to their school loan laptop if they have first gained permission from the ICT Technician.

- Use of the Internet on the school network during school contact hours must be for your professional duties only. At all other times internet use must be appropriate, and should not include financial transactions.

- Accessing (including viewing or showing to others) websites on the school network or on school owned ICT equipment which contains inappropriate or illegal materials is strictly forbidden and could result in dismissal.

- Downloading or printing material from websites on the school network or on school owned ICT equipment which contain inappropriate or illegal materials is strictly forbidden and could result in dismissal.

- Use of personal e-mail during school contact hours is prohibited.

- Use of file sharing activity on the school network or on school owned ICT equipment is strictly forbidden.

- E-mailing from the school network beyond the school should be through your Office 365 account or North Somerset Email Account

- Users are responsible for all e-mails sent, and for contacts made to those who may then e-mail back into the network.

- Unsolicited e-mails and unknown attachments must not be opened but deleted.

- Creating, circulating, viewing, showing to others and / or forwarding inappropriate, illegal or defamatory material, via email or uploading to websites, is strictly forbidden and could result in dismissal.

- Confidentiality of all material on the school network must be respected.

- Awareness and knowledge of children's AUP to follow guidance for accidental access of inappropriate material.

- Digital photos and moving images of children should only be taken as part of school life and learning activities.

- All staff must be sensitive to the taking and storing of digital photos or moving images of both learners and adults. The rights and wishes of children or adults whose images have been captured must be respected.

- Staff must be aware of which children should not have their photo (or other image) uploaded to the school website or to newspapers at their parents request. This extends to all websites.

- Digital photos or moving images of children should be stored in a labelled folder on staff laptops, cameras or the school network NOT on personal cameras, mobile phones or computers.

- Copyright of materials must be respected. Infringing copyright law is illegal.

- If you have used in your own teaching resources links to images, text and other material which is covered by copyright, then the source(s) must be acknowledged.

- The school reserves the right to monitor each user's internet use, and to examine or copy or delete any files which are held on the network or any other school owned ICT equipment.

- All adults in school have a duty of care to report to the Headteacher, or Chair of Governors, in confidence, if they have witnessed or suspect any inappropriate or illegal activity by any person on the school network or the internet.

- Appropriate security settings should be in place for use of social networking sites, so to protect professional identity and the safety of pupils.

- School business, dialogue or opinions regarding pupils and colleagues must not be shared digitally via social networking sites or email.

- This also is relevant to all ipad use

Report to the Headteacher, E-safety co-ordinator or Chair of Governors, immediately if:

- you are concerned about anything to do with the school ICT infrastructure, internet, or email.

- you are concerned you have unwittingly infringed a rule in this agreement.

Sanctions

Infringement of the Acceptable Use Agreement will be taken seriously.

In cases of serious misuse legal advice would have to be taken which could lead to a reprimand or dismissal or legal action.

Agreement

I have read and understood this Acceptable Use Agreement and agree to abide by it.

Name : ……

Signed: ……

Date: ……

APPENDIX 3

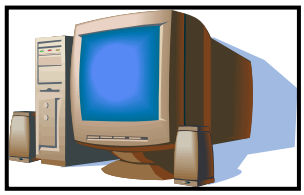
Our ICT Rules

Our ICT rules help us to enjoy using computers and they keep us safe.

I can use the computer if I have planned to do so.

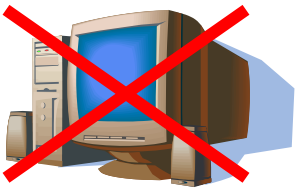
I will always be very careful with computers and ICT equipment when I am using it.

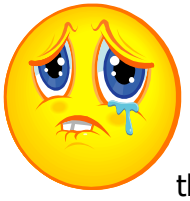
If I am not careful I will not be able to use the



computers.

I will tell an adult if something comes up on the screen that I do not understand, or upsets me.





Signed (child)**: . . . . . .**

Signed (parent)**: . . . . . .**

APPENDIX 4

Baytree School

Rules for acceptable use of ICT and the internet.

Our ICT rules help us to enjoy using computers and they keep us safe.

I will ask my teacher if I want to use the computer.

I will only use programs or websites that my teacher has told me to use.

I will ask my teacher if I want to do something new or different on the computer.

I will take care of the computer and other ICT equipment.

I will not click on keys or links, if I don't know what they do.

I ask for help from an adult if I am not sure what to do or if I think I have done something wrong.

I tell an adult if I see something unexpected or that upsets me on the screen.

If I break the rules I could lose Reward Time or I will miss my turn on a computer.

Signed (child):……

Signed (parent): ……..

APPENDIX 5

Baytree School

PUPIL RULES FOR ACCEPTABLE USE OF ICT AND THE INTERNET

ICT AT Baytree SCHOOL

At our school we believe that ICT and the Internet are very positive and powerful tools which helps the teaching you receive and your learning. ICT can make ideas clearer, it can make learning quicker, it can be fun, creative, and be enjoyed either when working by yourself or with others.

At Baytree we have computers, laptops, exciting software, digital cameras, video cameras, other special ICT equipment, Ipads and Internet access which can all be used for teaching and learning. Sometimes your teacher will tell you how to use these tools, and sometimes you will be encouraged to use them creatively by yourself or in a small group.

WHY WE NEED RULES FOR THE ACCEPTABLE USE OF ICT AND THE INTERNET IN SCHOOL

Our school wants you to be able to use ICT and the Internet creatively, responsibly and independently. These rules help you learn what you can do, and what you must not do, when using ICT and the Internet in school. They also help you to learn how to behave when out of school. Following the rules protects ICT equipment from damage, and keeps everyone safe and happy in school.

RULES FOR TAKING CARE OF ICT EQUIPMENT

- I will always be very careful when using any ICT equipment.
  I understand that ICT equipment is fragile and expensive.
  I will carry portable ICT equipment such as cameras and laptops carefully with both my hands.

- I will not fiddle with anything connected to the computer.
  I will always leave a computer and ICT equipment as I found it.

- I will only log on to the computer network with my own username and password.
  I will not share my login details with anyone outside school.

- I will not change any settings on the computer without permission from my teacher.
  I will report any warning messages I see on the screen to an adult.
  I will not attempt to by-pass the school's internet filtering system.

- I will not bring floppy disks, CD ROMs or data-sticks into school without teacher permission.
  If I have permission, I only use them on a computer when my teacher is with me.

RULES FOR KEEPING MYSELF AND OTHERS HAPPY AND SAFE AT SCHOOL WHEN USING ICT EQUIPMENT, THE INTERNET AND EMAIL

- I will only use the internet and email when given permission and supervised by my teacher.

- I must ask for permission to search the internet.
  I will tell my teacher what I am searching for, and the words I am using to search with.

- I will only look at or download material from the internet that is appropriate to the work I am doing.

- If I see something on the computer or internet that is inappropriate or upsets me, either at school or at home, I will report it to an adult immediately. Unfortunately this can happen by accident and telling an adult can stop it happening again.

- I will only send emails to people approved by my teacher.
  I will only send messages that are polite and friendly.
  I will not open emails or attachments from people I do not know.
  I will immediately report to my parent or teacher any upsetting or bullying messages sent to me at school or at home.

- When using the internet or email, I will not give out my personal details or the personal details of anyone I know at school or at home. (*This includes full names, date of birth, house addresses, email/msn addresses, telephone numbers, name of my school, photos of myself or friends and family, banking details, diary dates*).

- I will not attempt to use instant messaging or social networking sites at school. These sites are blocked by the school's filter.

- I will never arrange to meet a stranger through the internet or email.

- On a computer or using the internet at both school or at home I will not:

  * create…
  * show to others on screen…
  * photocopy…
  * send…
  * forward / pass on…

  …any material that would offend, upset or bully other children or adults at the school. (*This includes text, pictures, photos, video clips, animations, sound files or any other*

media)

- I understand that the school takes very seriously the cyber-bullying of any child or adult and must take strong action against it.

- I understand that writing or sending hateful / threatening messages which upset others is illegal.

- I will not upload any material on to the internet without my teacher first checking the content and giving me permission.

- I will respect the copyright of any material posted by others on the internet. If I use information from a website in my own work I will type the web address on my work.

- I will not break the school's copyright by using the school logo, letterhead, or any other material produced by the school on paper, its network or website without permission.

- I will only use school digital and video cameras when given permission and supervised by my teacher.
  I will only take appropriate photos or video clips of others or myself.
  I will respect the photos or video clips I have taken of others, and only use these in my work at school.

- The school discourages children bringing mobile phones (or other hand held devices) into school.
  If I have a mobile phone or device I will keep it turned off whilst on the school premises (this includes the playgrounds and playing fields) and leave it in the school office during the day.

- I understand that everything I create or look at on a computer leaves a 'digital footprint' that can be traced.
  I understand that the school monitors my use and can check my computer files and the websites I visit at any time.

TELL AN ADULT WHO WORKS IN SCHOOL STRAIGHT AWAY IF:

- **YOU ARE WORRIED ABOUT ANYTHING TO DO WITH THE INTERNET OR ICT.**

- **YOU ARE WORRIED YOU MAY HAVE BROKEN A RULE.**

THE ADULT WILL LISTEN TO YOU AND HELP SOLVE YOUR PROBLEM.

IF I BREAK THE RULES:

I understand that if I break these rules on purpose one or more of the following will happen:

- a verbal warning.

- not being able to use a computer or ICT equipment for a period of time set by my teacher.

- if it is serious you will be asked to speak to Mr Bowen-Roberts about your behaviour, and your parents will be informed.

- if it is very serious Mr Bowen-Roberts will have to act immediately and ask your parents or carers, to come into school. At this meeting your behaviour and the sanctions which may need to be taken will be discussed. If it is *extremely* serious and you have broken the law a police officer will have to be present at the meeting.

PUPIL AGREEMENT

Name: .....

I agree to keep these rules for the acceptable use of ICT and the Internet at Baytree School.

I understand the sanctions that will be used by the school if I break these rules.

Signed (child) : ..... Date: .....

Signed (parent): ..... Date: .....

APPENDIX 6

Baytree School

ACCEPTABLE USE AGREEMENT FOR THE INTERNET, E-MAIL AND SCHOOL ICT NETWORK & EQUIPMENT

Adult Visitors

- Children should only use the Internet supervised, and all weblinks checked prior to the lesson.

- Access to the network should only by made through your authorised account using your own username and password. This should be kept secret by yourself and the network administrators.

- Use of the Internet on the school network during school contact hours must be for your professional duties only. At all other times internet use must be appropriate, and should not include financial transactions.

- Accessing (including viewing or showing to others) websites on the school network or on school owned ICT equipment which contain inappropriate or illegal materials is strictly forbidden and could result in dismissal.

- Downloading or printing material from websites on the school network or on school owned ICT equipment which contain inappropriate or illegal materials is strictly forbidden and could result in dismissal.

- Creating, circulating, viewing, showing to others and / or forwarding inappropriate, illegal or defamatory material, via email or uploading to websites, is strictly forbidden and could result in dismissal.

- Confidentiality of all material on the school network must be respected.

- Digital photos and moving images of children should only be taken as part of school life and learning activities.

- Staff must be aware of which children should not have their photo (or other image).

- Digital photos or moving images of children should be stored in a labelled folder on staff laptops or the school network.

- Volunteers, students and supply staff must ask permission from their school based mentor, and temporary teaching and non-teaching staff from the Headteacher, if they wish to use digital images of children from Baytree beyond the school.

- Copyright of materials must be respected. Infringing copyright law is illegal.

- If you have used in your own teaching resources links to images, text and other material which is covered by copyright, then the source(s) must be acknowledged.

- All adults in school have a duty of care to report to the Headteacher, or Chair of Governors, in confidence, if they have witnessed or suspect any inappropriate or illegal activity by any person on the school network or the internet.

Report to the Headteacher, immediately if:

- you are concerned about anything to do with the school ICT infrastructure, internet, or email.

- you are concerned you have unwittingly infringed a rule in this agreement.

Sanctions

Infringement of the Acceptable Use Agreement will be taken seriously.

In cases of serious misuse legal advice would have to be taken which could lead to a reprimand or dismissal or legal action.

Agreement

I have read and understood this Acceptable Use Agreement and agree to abide by it.

Name : ……

Signed: ……

Date: ……

APPENDIX 7

Baytree School

SCHOOLS' SOCIAL MEDIA/NETWORKING POLICY

OVERVIEW AND INTRODUCTION

1.1 The purpose of this policy is to:

- Ensure Baytree school (henceforth known as 'the school') exposure to legal and governance risks is minimises;
- Enable workers at the school to use social networking sites safely and securely (Social Networking sites can be in school depending on what the school's Policy is (see Section 4 below)
- Ensure that workers are aware of their responsibilities in connection with the use of social networking sites and any impacts in relation to their employment
- Ensure that workers are aware of the risks associated with the inappropriate use of social networking sites – and how this may impact on their employment
- Safeguard workers at the school in connection with the use of social networking sites and minimise the risk that they make themselves vulnerable
- Ensure the Governing Body maintains its duty to safeguard children, the reputation of the school and those who work for it, the wider community and the Local Authority.

SCOPE AND GENERAL PRINCIPLES

2.1 In this Policy 'worker' means all individuals engaged by the school in a paid or voluntary capacity including governors, those on work experience placements and agency workers. Third parties acting on behalf or in partnership with the school are also expected to adhere to this guidance.

2.2 This Policy applies to social networking sites, personal web pages, personal space provided by internet providers and internet presences which make available personal information/opinions to the general public including but not limited to Facebook, Bebo, MySpace, Windows Live Spaces, MSN, Twitter, YouTube, blogs, wikis, forums, bulletin boards, chatrooms, multiplayer on-line gaming, virtual worlds and instant messenger.

2.3 In this Policy 'pupil' should, where relevant, be taken to include any child/young person attending the school. If an employee has a difficulty complying with this requirement (for example if they are related to a pupil attending the school) they should declare this relationship to the Headteacher/school designated safeguarding teacher.

2.4 The Governing Body does not discourage workers at the school from using social networking sites. However, all workers at the school should be aware that the Governing Body will take seriously any occasions where the services are used

inappropriately. If there are allegations of online bullying or harassment, these will be dealt with in the same way as other such instances.

2.5 In the event that this Policy is not followed or any instances of the inappropriate use of social networking sites are brought to the attention of the School, these may be investigated under the School's Disciplinary Policy and, depending on the seriousness of the matter, disciplinary action may be taken which may result in dismissal.

2.6 Where there are concerns as to the legality of any activity or behaviour or any allegations which have a children's safeguarding dimension the School or Local Authority will be obliged to inform the police.

RESPONSIBILITIES

3.1 The Governing Body shall:

- Ensure this policy is implemented and procedures are in place that deal with the use of social networking sites
- Ensure that all workers at the school have access to this policy and that workers including new workers are made aware of it

3.2 Headteachers/Line Managers shall:

- Be familiar with this policy and guidelines and ensure that workers understand the policy and their own responsibilities
- Ensure that workers at the school are aware of the risks of the use of social networking sites and the possible implications of the inappropriate use of them
- Make partners and any other third parties aware of this guidance where relevant
- Instigate disciplinary procedures where appropriate to do so
- Seek advice where necessary from Human Resources on the approach to be adopted if they are made aware of any potential issue

3.3 Workers at the school shall:

- Behave responsibly and professionally at all times in connection with the use of social networking sites
- Ensure that all communication with pupils (including on-line communication) takes place within clear and explicit professional boundaries as set out in the *DfE Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings*.
- Raise any concerns that any colleague(s) is/are not acting in accordance with this Policy with their line manager/the headteacher/safeguarding officer.
- Use their professional judgement and, where no specific guidance exists, take the most prudent action possible and consult with their manager or the headteacher if they are unsure
- Co-operate with management in ensuring the implementation of this policy
- Respect the privacy and feelings of others
- Keep a professional distance from pupils and ensure a clear separation of the private social lives of workers at the school and those of pupils
- Report to their Headteacher or line manager any occasions when a pupil attempts to involve them in on-line or social networking activity

3.4 Parents and third parties are encouraged to:

- Raise any concerns that any worker(s) at the school is/are not acting in accordance with this Policy with the headteacher

USE OF SOCIAL NETWORKING SITES

4.1 All workers at the school should follow the following guidance/procedures: (*Please note: if a worker at the school believes they will have any difficulty complying with any of the requirements below for whatever reason (for example : where they are related to a pupil), they should discuss the matter with the Headteacher. Failure to do so will be regarded as a serious matter.*

1. Workers at the school must not access social networking sites for personal use via school information systems or using school equipment
2. Workers at the school must not accept pupils as friends or use internet or web-based communication channels to send any personal messages to pupils – personal communication could be considered inappropriate and unprofessional and makes workers at the school vulnerable to allegations
3. Workers at the school are advised not to be friends with recent pupils (the potential for workers at the school to be compromised in terms of content and open to accusations makes the risk not worth taking) and workers at the school are also advised not to be friends with pupils at other schools as this is likely to make them vulnerable to allegations and may be open to investigation by the Local Authority or police. Where a worker is considering <u>not</u> following this advice, they are required to discuss the matter, and the implications with the Headteacher.
4. Any student-initiated communication, on-line friendships/friend requests must be declined and reported to the Headteacher or designated children's safeguarding teacher/officer. (If a worker receives messages on his/her social networking profile that they think could be from a pupil they must report it to their line manager/headteacher and discuss whether it is appropriate to contact the internet service or social networking provider so that they can investigate and taken the appropriate action)
5. Workers at the school should not share any personal information with any pupil (including personal contact details, personal website addresses/social networking site details)
6. Workers at the school should not place/post any material (or links to any material) of a compromising nature (that is, any material a reasonable person might find obscene or offensive (such as sexually explicity or unlawfully discriminatory material) including inappropriate photographs or indecent remarks or material relating to illegal activity) on any social network space
7. Workers at the school are advised not to write about their work but where a worker at the school chooses to do so, he/she should make it clear that the views expressed are his/hers only and do not reflect the views of the school/Local Authority (and all other guidelines in this policy must still be adhered to when making any reference to the workplace)

8. Workers at the school must not disclose any information that is confidential to the school or disclose personal data or information about any individual/colleague/pupil, which could be in breach of the Data Protection Act or disclose any information about the school/Local Authority that is not yet in the public arena
9. Workers at the school should not post photographs of pupils under any circumstances and should not post photographs of colleagues or parents without their express permission
10. Workers at the school should not make abusive/defamatory/undermining/derogatory remarks about the school/colleagues/pupils/parents/governors or the Local Authority or post anything that misrepresents or could potentially bring the school/Local Authority into disrepute
11. Workers at the school should not disclose confidential information relating to their employment at the school
12. Workers at the school must not link their own sites to the school website or use the school's or the Local Authority's logo or any other identifiers on their personal web pages
13. If any worker at the school receives media contact regarding the content of their site or is offered payment for site content which relates to the school they must consult their headteacher/line manager
14. No worker at the school should use any internet/on-line resources to seek information on any pupil, parent or other worker at the school other than for the purposes of legitimate monitoring of the usage of Social Networking sites by designated managers/officers
15. Workers at the school should not use social networking sites to seek to influence pupils regarding their own political or religious views or recruit them to an organisation of this kind using their status as a trusted adult to encourage this.

4.2 All communication via social networking sites should be made with the awareness that anything said, shown or received could be made available, intentionally or otherwise, to an audience wider than that originally intended. Workers at the school are strongly advised, in their own interests, to take steps to ensure that their on-line personal data is not accessible to anybody who they do not want to have permission to access it. For example, they are advised to check the security and privacy settings of any social networking site they subscribe to and set these to a maximum. For further information see the safer internet website
http://www.safeinternet.org.uk and the South West Grid for Learning Resources
http://www.swgfl.org.uk/Staying-Safe

4.3 The School reserves the right to take action to obtain the removal of any content posted by workers at the school which may adversely affect the reputation of the school or put it at risk of legal action

4.4 We would expect all former colleagues at the school to continue to be mindful of good children's safeguarding practice and of the school's reputation in using social networking sites.

USE OF SCHOOL SITES, PAGES AND SPACES

5.1 All workers at the school should follow the following guidance/procedures:

1. The School ICT Policy must be adhered to at all times when content is posted on the school sponsored sites/pages/spaces or on-line school communication systems/networks are used. Any breach in this regard will result in the offending content being removed and may result in disciplinary action and any 'publishing' rights of the relevant worker being suspended in accordance with the Schools ICT Policy
2. Communications or pages undertaken/run on behalf of the school must be password protected and run from the school website
3. Workers at the school must not run social network spaces for student use on a personal basis. If a network is to be used to support students with coursework and as part of the educational process, professional spaces must be created by workers and pupils using a restricted, school-endorsed networking platform in line with school ICT and governance policies. (Specific sites can be negotiated via a licence process for relevant colleagues, with specific guidelines being set out and backed by a signed undertaking from the relevant colleagues to use the sites in accordance with the guidelines).
4. Any inappropriate behaviour by pupils on-line must be reported to the Headteacher or member of the senior leadership team and will be dealt with through the school's pupil disciplinary process
5. Workers at the school should not request or respond to any personal information from any pupil unless consistent with their professional role and approved by the school

EQUAL OPPORTUNITIES

6.1 Managers must not discriminate on the grounds of race, age, gender, disability, sexual orientation, religion or belief, gender reassignment, marriage and civil partnership, pregnancy and maternity, or other grounds and ensure that the needs of workers are given careful consideration when applying this Policy.

RELEVANT POLICIES/GUIDANCE

- Disciplinary Policy and Procedure
- Code of conduct
- Children's Safeguarding Guidance
- Equality Scheme/Policy
- ICT Policy/Acceptable Use Policy
- E-Safety Policy

LEGISLATION

The following legislation must be considered when adhering to this policy:

- Obscene Publications Act 1959
- Protection of Children Act 1988
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006

- Defamation Act 1996
- Protection from Harassment Act 1997
- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act (RIPA) 2000
- Safeguarding Vulnerable Groups Act 2006
- Equality Act 2010

Agreement
I have read and understood this Social Media/Networking Policy and agree to abide by it.

Name : ……

Signed: ……

Date: ……

APPENDIX 8

Baytree School

Personal Data Policy

October 2012

Introduction

Baytree School will do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of Baytree school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

Have permission to access that data
Need to have access to that data

Any loss of personal data can have serious effects for individuals and/or institutions concerned, can bring the school into disrepute and may well result in disciplinary action and/or criminal prosecution. All transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant legislation and relevant regulations and guidance from the Local Authority.

The Data Protection Act (1998) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow 'good information handling principles'.

Policy Statements

Baytree School will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed.

Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the 'Fair Processing Code' and lawfully processed in accordance with the 'Conditions for Processing'.

Personal Data

Baytree school and visiting Professionals/Governors will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an

individual and provides specific information about them, their families or circumstances. This will include:

Personal information about members of the school community – including puipils, members of staff and parents and carers eg names, addresses, contact details, legal guardianship/contact details, health records, disciplinary records

Curricular/academic data eg class lists, pupil progress records, reports, references

Professional records eg employment history, taxation and national insurance records, appraisal records and references

Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members

Responsibilities

Baytree School's Senior Information Risk Officer (SIRO) (Ed Bowen-Roberts). The SIRO will keep up to date with current legislation and guidance and will:

Determine and take responsibility for the school's information risk policy and risk assessment

Work with the Information Asset Owners (IAOs) (Carolynne Smyth/Issy Johnson/Jackie Rawle/Cara Richards)

The school will identify Information Asset Owners (IAOs) for the various types of data being held (eg pupil information, staff information/assessment data etc). The IAOs will manage and address risks to the information and will understand

What information is held and for what purpose
How information has been amended or added to over time
Who has access to protected data and why

Everyone in Baytree has the responsibility of handling protected or sensitive data in a safe and secure manner.

Display equipment must be positioned so that the screen display is not visible to any unauthorised persons.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

Baytree School is registered as a Data Controller on the Data Protection Register held by the Information Commissioner (this is renewed each year in January by the Bursar and costs £35).

Information to Parents/Carers – the 'Privacy Notice'
Under the 'Fair Processing' requirements in the Data Protection Act, the school will inform parents/carers of all pupils/students of the data they hold on the pupils/students, the purposes for which the data is held and the third parties (eg LA, DCSF, QCA, Connexions etc) to whom it may be passed. This privacy notice is passed to parents/carers and is available on the schools website. Parents/carers of young people who are new to the school will be provided with the Privacy Notice on joining the school.

Training and Awareness
All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through:

Induction training for new staff
Staff meetings/briefings/Inset
Day to day support and guidance from Information Asset Owners

Identification of Data
The school will ensure that all school staff, contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher.

Secure Storage of and access to Data
Baytree School will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.

All users will be given secure user names and strong passwords which must be changed regularly. User names and passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.
All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media). Private equipment (ie owned by the users) must not be used. When personal data is stored on any portable computer system, USB stick or any other removable media:

The data must be encrypted and password protected
The device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected
The device must offer approved virus and malware checking software

The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups)

All paper based material must be held in lockable storage.

The school recognises that under Section 7 of the Data Protectin Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests ie a written request to see all or part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them, a description of that data, the purpose for which the data is processed, the sources of that data, to whom the data may be disclosed, and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification, blocking, erasure and destruction of data.

Secure transfer of data and access out of school
Baytree school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

Users may not remove or copy sensitive or personal data from the school , or transferred premises without permission from a member of the SLT and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school.
When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
Users must protect all portable and mobile devices, including media,used to store and transmit personal information using approved encryption software.
Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be
taken from the local authority in this event after gaining permission from a member of the SLT.

Disposal of Data
Baytree School will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely

overwritten, in accordance with Government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data – advice on how to do this to be sought from the ICT Co-ordinator or IT Support Richard Perry.

Audit Logging/Reporting/Incident Handling

As required by the 'Data Handling Procedures in Government' document, the activities of data users, in respect of electronically held personal information, will be logged and these logs will be monitored by the SLT.

The audit logs will be kept to provide evidence of accidental or deliberate security breaches – including loss of protected data or breaches of an Acceptable Use Policy, for example. Specific security events should be archived and retained at evidential quality for seven years.

Baytree School has a Critical Incident Policy for reporting, managing and recovering from information risk incidents, which establishes

A 'Responsible person' for each incident
A communications plan, including escalation procedures
And results in a plan of action for rapid resolution and
A plan of action of non-recurrence and further awareness
Raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Joint Campus Policy for Mobile Phone Around Pupils
May 2012

This policy applies to all Campus staff and contractors and visitors* whilst they are in areas used by children.

Staff (contractors or visitors) must not use or have their mobiles with them when they are working with or supervising children, or in public areas eg classrooms, corridors, reception areas.

Staff (contractors or visitors) must not give their personal contact details (eg personal mobile phone no, personal e-mail or social networking details) to pupils or families of pupils.

Staff (contractors or visitors) must not let pupils use their personal mobile phones.

Staff (contractors or visitors) must not allow pupils to be "friends" on Facebook or other social networking sites.

Staff (contractors or visitors) must not use their personal mobiles to contact parents/carers.

Staff (contractors or visitors) must not use their personal mobile to take photos or video of pupils.

Staff, with prior arrangement of their Headteacher can use personal cameras within school. This is with the understanding that the Headteacher can request to view the photos/video that have been taken. All images must only be stored on a school owned computer.

In the event of an emergency occurring whilst off-site with pupils, staff should use their personal mobile (in the event of not having a school or campus mobile phone) to contact the emergency services if needed and then contact their school (or campus) reception. The school administration team will ensure that all parents/carers are contacted and pass on the information.

*Contractors and visitors
Contractors and visitors will be asked not to use their phones in pupil areas, this includes corridors.

Contractors and visitors must never take photos or video of pupils using their mobile phones.