Blackshaw Moor CE (C) First School
ICT Policy

Rationale: Over recent years there has been an ICT revolution and computers are now an essential part of our society. We intend to use ICT as a tool to enhance and develop the curriculum. We will also help pupils become knowledgeable about the nature of information, comfortable with new technology and able to exploit its potential. We feel it is an essential part of a child's school experience.

Purpose: This policy aims to show how our school intends to fulfil its legal obligation to deliver the National Curriculum – ICT – and how we can go beyond that to create a stimulating and exciting curriculum which will meet the needs of our children.

Guidelines: Aims
Teaching and Learning
Early Years Foundation Stage
Planning
Cross-curricular Links
Access
Assessment and Recording
Resources
Equal Opportunities
SEN

Appendix: Internet policy
List of Hardware/ Software
E-safety policy
Dyslexia Friendly statement
AU Policy

Conclusion: This policy should have a positive effect on the teaching and learning of ICT in the school by encouraging a consistent approach throughout the school.

Agreed by staff……………………. Agreed by Governors…………………

Introduction

ICT is the technology associated with the handling of information. It involves learning about and using a wide range of devices that store and transmit information. It includes the use of computers to store and communicate information, to control mechanical devices and to provide real life models or simulations for children to investigate.

Aims

Blackshaw Moor School seeks to:

- Present ICT as a creative and fascinating process in which children are encouraged to use their own imaginations, initiative, reasoning and investigative skills.
- Stimulate interest in new technologies, develop ICT skills, provide all pupils with their National Curriculum entitlement, help our pupils acquire confidence and pleasure in using ICT, become familiar with some everyday applications and be able to evaluate technology's potential limitations.
- Enrich and extend learning throughout the curriculum using the technology to support collaborative work and independent study.
- Help pupils appreciate the relevance of ICT in our society and use it as a tool for learning and investigation in all subjects.
- Use the power of the technology to help pupils with special educational needs or physical disabilities to increase their independence and develop their interests and abilities.
- Encourage the flexibility and openness of mind necessary to adjust to, and take advantage of, the ever – quickening pace of technological change.

Teaching and Learning

We recognise that the computer is a scarce resource and intend to make the best possible use of it. We believe children can achieve National Curriculum levels of attainment and important ICT skills through short but frequent use of the computer rather than lengthy tasks.

These machines are in one area of each classroom so that a small group can work on the same task simultaneously and so ICT is now planned into the daily Literacy and Numeracy lesson for a group of children, if appropriate. Each classroom has an interactive smart whiteboard.

We feel it is important to regard ICT as a discrete subject and so alongside this we have an ICT teacher who can then teach specific skills such as general keyboard skills, text editing, data and graphic skills and computer coding which is a larger part of the new computing curriculum.

Where possible we teach ICT to the whole class and we have invested in new technology, such as remote keyboards and interactive white boards, to make this easier.

Early Years Foundation Stage

The Early Years class has an interactive whiteboard. The children use the PC as a free choice activity and a more structured use, when they are introduced to early skills such as mouse control, selecting and loading programmes, is included in weekly planning. ICT, where appropriate, is included in daily literacy and numeracy plans. The school is at the stage of developing the website as a communication tool between home and school and as a way for children to develop new ICT skills at school and also away from the classroom.

Planning

We have a scheme of work produced by Entrust that outlines software to be used and skills and knowledge to be taught in each year group. This ensures continuity and progression throughout the key stages.

Access

To ensure maximum access for all pupils, there are laptops in each classroom. The class teacher will use the technology with the pupils to encourage the use of ICT across the curriculum. At present no pupils need specialist equipment to use a PC.

Assessment and Recording

Each child has their own folder on each computer to store examples of their work on. We feel this is important, as the children will be involved in recording their own progress. In addition each child has an ICT folder to store printed copies of work. The class teacher and ICT teacher are responsible for assessing and monitoring progress. Knowledge and skills to be assessed are described in medium term plans and the ICT teacher makes evaluations that are recorded on weekly planning. Children's progress is then recorded at the end of the unit and tracked over the year.

Resources:

At present we have no leased computers.

Our development plan is updated yearly and contains information about hardware and software we feel is required. Funding for replacing machines is provided when necessary.

Equal Opportunities

There is a commitment to provide equal opportunities for all pupils. All ICT is planned to ensure equal interest and involvement by all children regardless of gender or ability.

SEN

Children who find it difficult to present work and leave spaces sometimes use a word processor.

We have certain English programmes such as *Wordshark* and Literacy, Numeracy Bank which specifically help children with dyslexic tendencies to improve their spelling.

ICT and Dyslexia

At Blackshaw Moor we believe the use of ICT can be used effectively to support the learning of children with Dyslexia.

We will use comic sans font on the interactive white boards and change the background colour from white when presenting information to the whole class.

Clicker is a useful wordbank to support children when writing in other subject areas and Talking First word can be used to listen to written instructions.

We use the ORT series of Literacy Box and Rhyme and Analogy to support the acquisition of key literacy skills and also Wordshark to develop phonological awareness and spelling skills.

Subject teachers of ICT should refer to Appendix 1 : ICT and Dyslexia – IDP training materials for specific guidance on how to use ICT to support children with Dyslexia

E-safety Policy Document Blackshaw Moor CE(C)) First School

Introduction

This broader policy will include Our Internet Safety Policy and an Acceptable Usage policy covering all technologies and issues relevant to our school. In it we will detail how we as a school intend to keep our pupils safe when using Information and communication technologies.

Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students / pupils* to take a responsible approach. The education of *students / pupils* in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.
E-Safety education will be provided in the following ways:

A planned e-safety programme will be provided as part of ICT / PHSE and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.

- Key e-safety messages will be reinforced as part of a planned programme of assemblies and an annual e-safety day to keep the issue firmly in everyone's attention.
- Pupils will 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

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 during a staff meeting.
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings on a regular basis.
- The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required

Governors

Governors will be made aware of e-safety issues through curriculum committee meetings. The governors with reponsibilty for ICT and child protection will be made aware of e- safety issues through

- Participation in school training / information sessions for staff or parents

Curriculum

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, we feel it is best practice that pupils should be guided to sites checked as suitable for their use. We do have a comprehensive filtering system in place. However if this did fail and unsuitable sites were displayed this must be reported immediately to the ICT coordinator who will add it to the filter list.
- Where Pupils are allowed to freely search the internet, eg using search engines, staff will be vigilant in monitoring the content of the websites the young people visit.
- Pupils will 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
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet and to be aware of the potential consequences of plagiarism.

. We also have a monitoring solution installed and our own netwoek by the PCE. It monitors all activity on thenetwork and the IT co ordinator checks the reports fortnightly.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Becta advises that schools should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature (Becta – Good Practice in information handling in schools – keeping data secure, safe and legal – Sept 2008).

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

- have permission to access that data
- need to have access to that data.

We are aware that any loss of personal data can have serious effects for individuals and can bring the school into disrepute and may well result in disciplinary action and / or criminal prosecution. We realise that 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 data legislation and relevant regulations and guidance from the Local Authority.

Secure transfer of data and access out of school

The 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 authorised premises without permission 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) 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.

Disposal of data

The 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 (see further reading section for reference to the Cabinet Office guidance), and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

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 responsible individuals.

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.

The school has a 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.

Headteachers:

- 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 is responsible for ensuring that the E-Safety Coordinator receives suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant

- The Headteacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see SSCB website for a flow chart on dealing with e-safety incidents)

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, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety coordinator/ Headteacher
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils understand and follow the school e-safety and acceptable use policy
- Pupils 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 students / 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.

Designated person for child protection / Child Protection Officer

will be trained in e-safety issues and will 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

Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. (nb. at KS1 we would expect that parents / carers would sign on behalf of the pupils)
- 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, 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 every opportunity to help parents understand these issues through parents' evenings, newsletters, , website / information about national / local e-safety campaigns / offering e- safety awareness training in the autumn term. Parents and carers will be responsible for:

- **endorsing (by signature) the Student / Pupil Acceptable Use Policy**

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school.
- Images we use will only be shared on our school website and then only with parental responsibility.

- Pupil’s work can only be published with the permission of the student / pupil and parents or carers.

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:

Please tick ✓	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school		x						x
Use of mobile phones in lessons				x				
Use of mobile phones in social time	x							x
Taking photos on mobile phones or other camera devices				x		x (1)		
Use of hand held devices eg PDAs, PSPs				x				
Use of personal email addresses in school, or on school network				x				
Use of school email for personal emails				x				
Use of chat rooms / facilities				x				
Use of instant messaging				x				
Use of social networking sites				x				
Use of blogs		x (2)				x		

The school may also wish to add some policy statements about the use of communications technologies, in place of, or in addition to the above table:

Key: (1) e.g. school trip to).E.C Standon Bowers.
(2) Alllowed for school projects.

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 should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access). Although there are times when staff are working at home and will send and receive emails to and from the school system. Staff will not send any confidential material in an email unless it is password protected and on the school system.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – 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 students / pupils or parents / carers (email, chat, 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.*
- Where possible, whole class or group email addresses will be used by all classes.
- Students / pupils 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

Filtering and Monitoring

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. As a part of the Staffordshire Learning Network schools we automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

However no filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use agreement. Monitoring will take place using PCE. The e-safety coordinator will monitor internet usage at least once a month and report any violations and take appropriate action.