Brookfields Primary School E-Safety Policy

Our E-Safety Policy has been written by the school, building on the Birmingham LINK2ICT draft E-safety policy, SWGL policy guidance, BECTA and government guidance. It has been agreed by the School Leadership Team and approved by governors. It will be reviewed annually. It should be recognised that E-Safety is a whole school issue relating to Safeguarding and not specifically an issue of ICT.

Related Documents:
Acceptable Use Policy for Staff (AUP)
Acceptable Use Policy for pupils (AUP)
Behaviour Policy
Birmingham City Council Internet Use Policy, Internet Use Code of Practice and Email Use Policy (Linked from www.bgfl.org/esafety)

DSLs/E-safety coordinators: Dawn Benton and Jane Cross
Implementation Date: September 2015
Review Date: September 2016

Aims

This policy document sets out the school's aims, principles and strategies for using the internet and protecting pupils. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

Staff and pupils have access to web sites worldwide offering educational resources, news and current events. There will be opportunities for discussion and exchange of information within the school community and others worldwide. Staff have the opportunity to access educational materials and good curriculum practice, to communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the Local Authority, BEP, and Department for Education (DfE); receive up-to-date information and participate in government initiatives such as National Grid for Learning (NGfL) and the Virtual Teacher Centre. The internet is also be used to enhance the school's management information and business administration systems.

Roles and Responsibilities

The Head and Governors have ultimate responsibility for establishing safe practice and managing e-Safety issues at our school. Governors will nominate a lead governor for Computing. The role of DSLs/ E-safety coordinators has been allocated to Dawn Benton and Jane Cross, our designated senior leads for child protection and members of the senior management team. They are the central point of contact for all e-Safety issues.

All members of the school community have certain core responsibilities within and outside the school environment. They should:

- Use technology responsibly.

- Accept responsibility for their use of technology.
- Model best practice when using technology.
- Report any incidents to the DSL/Computing Lead using the school procedures.
- Understand that network activity and online communications are monitored, including any personal and private communications made via the school network.
- Be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action.

Publicising e-Safety

Effective communication across the school community is key to achieving the school vision for safe and responsible citizens. To achieve this we will:

- Make this policy, and related documents, available on the school website.
- Introduce this policy, and related documents, to all stakeholders at appropriate times. This will be at least once a year or whenever it is updated
- Display relevant e-Safety information in the ICT suite
- Provide e-Safety information at parents progress meetings and through the school Moodle

Physical Environment / Security

The school endeavours to provide a safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system consulting with the LA where appropriate.

- Sophos anti-virus software is installed on all computers and updated regularly
- Central filtering is provided and managed by Link2ICT. All staff and pupils understand that if an inappropriate site is discovered it must be reported to the Computing Lead who will report it to the Link2ICT Service Desk to be blocked.
- All incidents will be recorded in the E-Safety log for audit purposes.
- Requests for changes to the filtering will be directed to the ICT co-ordinator in the first instance who will forward these on to Link2ICT or liaise with the Head as appropriate. Change requests will be recorded in the e-Safety log for audit purposes
- The School uses Policy Central Enterprise on all school owned equipment to ensure compliance with the Acceptable Use Policies.
    - Pupils' use is monitored by the Head Teacher
    - Staff use is monitored by the Head Teacher
- All staff are issued with their own username for network access.
- Visitors / Supply staff will be issued with temporary ID's and the details recorded in the reception office
- All pupils are issued with their own username and understand that this must not be shared.

Mobile / Emerging Technologies

- Teaching staff at the school are provided with an ipad for educational use and their own professional development. All staff understand that the Acceptable Use Policies (AUP) apply to this equipment at all times.
- Pictures / videos of staff and pupils should not be taken on personal devices.
- New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community

E-mail

The school e-mail system is provided, filtered and monitored by Link2ICT is governed by Birmingham City Council E-mail Use Policy.

- All staff are given a school e-mail address (provided by Zimbra) and understand that this must be used for all professional communication
- Everyone in the school community understands that the e-mail system is monitored and should not be considered private communication
- Staff are allowed to access personal e-mail accounts on the school system outside directed time and understand that any messages sent using the school equipment should be in line with the e-mail policy. In addition, they also understand that these messages will be scanned by the monitoring software

Digital Media

- We respect the privacy of the school community and will obtain written permission from staff, parents, carers or pupils before any images or video are published or distributed outside the school.
- Photographs will be published in line with Becta guidance and not identify any individual pupil.
- Pupils' full names will not be published outside the school environment

Data Security / Data Protection

Personal data will be recorded, processed, transferred and made available in line with 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.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

Sensitive personal pupil/staff data should never be taken off site without permission. In instances where permission is given, the personal data that is stored on portable computer systems, USB sticks or any removable media should adhere to the following:

- The data must be encrypted and password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device once it has been transferred or its use is complete

Educational Use

- School staff model appropriate use of school resources including the internet.
- All activities using the internet, including homework and independent research topics, will be tested first to minimise the risk of exposure to inappropriate material

- Where appropriate, links to specific web sites will be provided instead of open searching for information pupils will be taught how to conduct safe searches of the internet as party of annual safety lessons provided by the Computer Lead.
- Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- Teachers will be responsible for their own classroom management when using computer equipment and will remind pupils of the Acceptable Use Polices before any activity
- Pupils 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

The Use of the Internet to Enhance Learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils’ age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

In common with other media such as magazines, books and video, 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 BCC can accept liability for the material accessed, or any consequences of Internet access.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Head teacher and Governors will ensure that the Internet policy is implemented and compliance with the policy monitored.

Pupil Consultation

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of 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 should be provided as part of Computing / PHSE / other lessons and should be regularly revisited – this will cover both the use of computers and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme of assemblies or lessons
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of computing, the internet and mobile devices both within and outside school

- Pupils and parents will sign the Internet/acceptable use policy (see appendix B)
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- 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
- The pupil acceptable usage agreement will be displayed in the computer suite.
- Pupils will be informed that Internet use will be monitored (Policy Central Enterprises)
- Instruction in responsible and safe use should precede Internet access.

Staff Consultation

- All staff must accept the terms of the 'Birmingham Education Service Policy for Acceptable use of the internet'
- Staff will ensure they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP). (See appendix B)
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by the Senior Leadership Team.
- All staff need have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- Staff must report any suspected misuse or problem to the Computing Lead/ DSL/ E-safety coordinator or Head teacher for investigation / action / sanction
- Digital communications with pupils (Virtual Learning Environment (VLE) should be on a professional level and only carried out using official school systems
- Staff 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 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.
- Staff's personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school's teacher handbook.

Responding to incidents

It is hoped that all members of the school community will be responsible users of computers, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity, i.e.

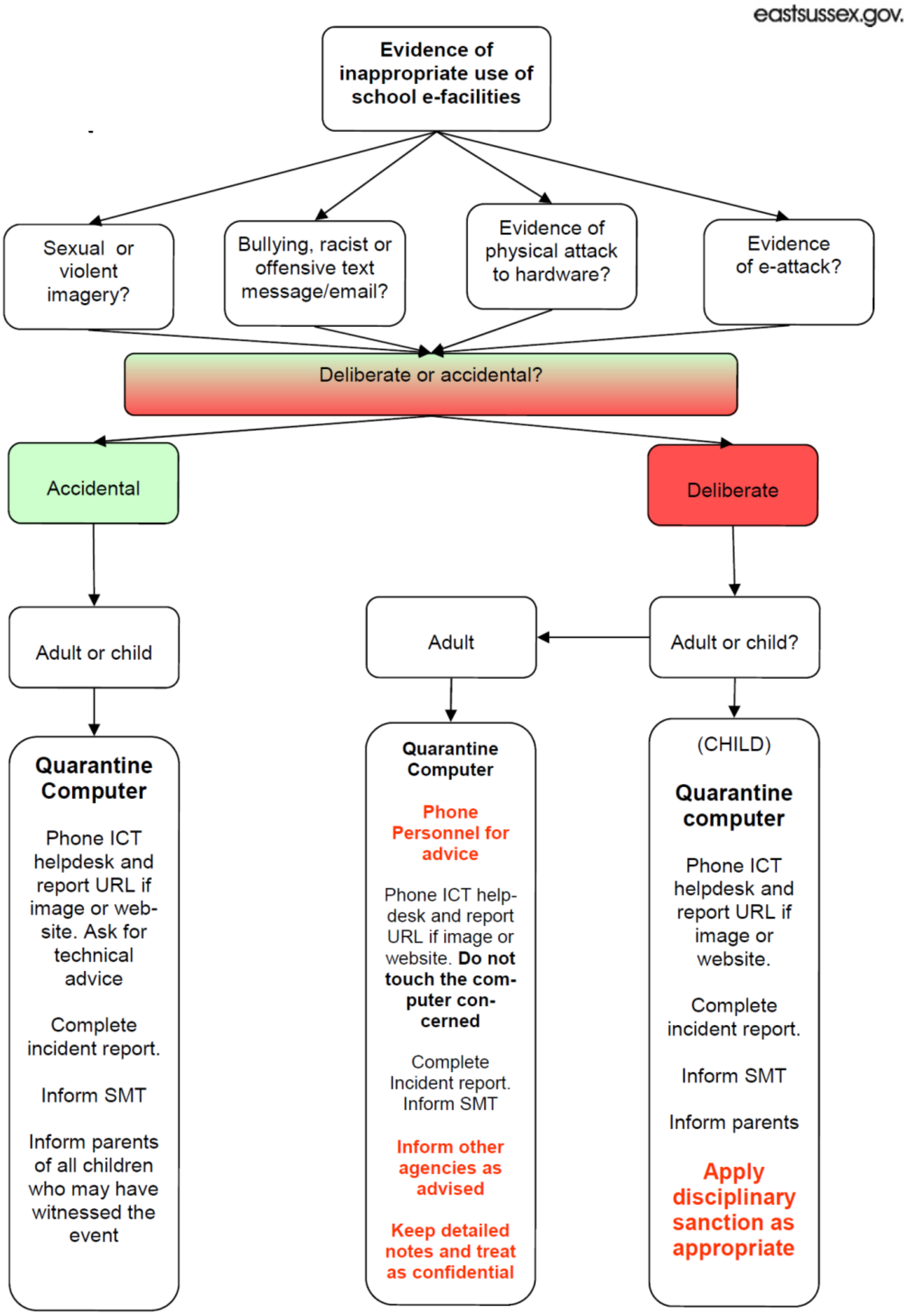
- **Child sexual abuse images**
- **Adult material which potentially breaches the Obscene Publications Act**
- **Criminally racist material**
- **Other criminal conduct, activity or materials**

- Inappropriate use of the school resources will be dealt with in line with other school policies e.g. Behaviour and Child Protection Policy.
- Any suspected illegal activity will be reported directly to the police. The Link2ICT Service Desk will also be informed to ensure that the Local Authority can provide appropriate support for the school
- Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be referred directly to the Head
- Breaches of this policy by staff will be investigated by the Head teacher. Action will be taken under Birmingham City Council's Disciplinary Policy where a breach of professional conduct is identified. Incidents will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct. All monitoring of staff use will be carried out by at least 2 senior members of staff.
- Pupil policy breaches relating to bullying, drugs misuse, abuse and suicide must be reported to the nominated safeguarding representative and action taken in line with school safeguarding policies. There may be occasions when the police must be involved.
- Serious breaches of this policy by students will be treated as any other serious breach of conduct in line with school Behaviour Policy. Referral to Heads of Phase may be appropriate at this level. Heads of Phase will also deal with email alerts generated by PCE for pupils. For all serious breaches, the incident will be fully investigated, and appropriate records made on personal files with the ultimate sanction of exclusion reserved for the most serious of cases.
- Minor Pupil offences, such as being off-task visiting games or email websites will be handled by the teacher in situ by invoking the school behaviour policy.
- The Educations and Inspections Act 2006 grants the Head teacher the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate (See flow chart to determine the right course of action)

East Sussex County Council

eastsussex.gov.uk

E–safety incident guidance for staff



Evidence of inappropriate use of school e-facilities

Sexual or violent imagery?

Bullying, racist or offensive text message/email?

Evidence of physical attack to hardware?

Evidence of e-attack?

Deliberate or accidental?

Accidental

Adult or child

Quarantine Computer

Phone ICT helpdesk and report URL if image or website. Ask for technical advice

Complete incident report.

Inform SMT

Inform parents of all children who may have witnessed the event

Deliberate

Adult or child?

Adult

Quarantine Computer

Phone Personnel for advice

Phone ICT helpdesk and report URL if image or website. **Do not touch the computer concerned**

Complete Incident report. Inform SMT

Inform other agencies as advised

Keep detailed notes and treat as confidential

(CHILD)

Quarantine computer

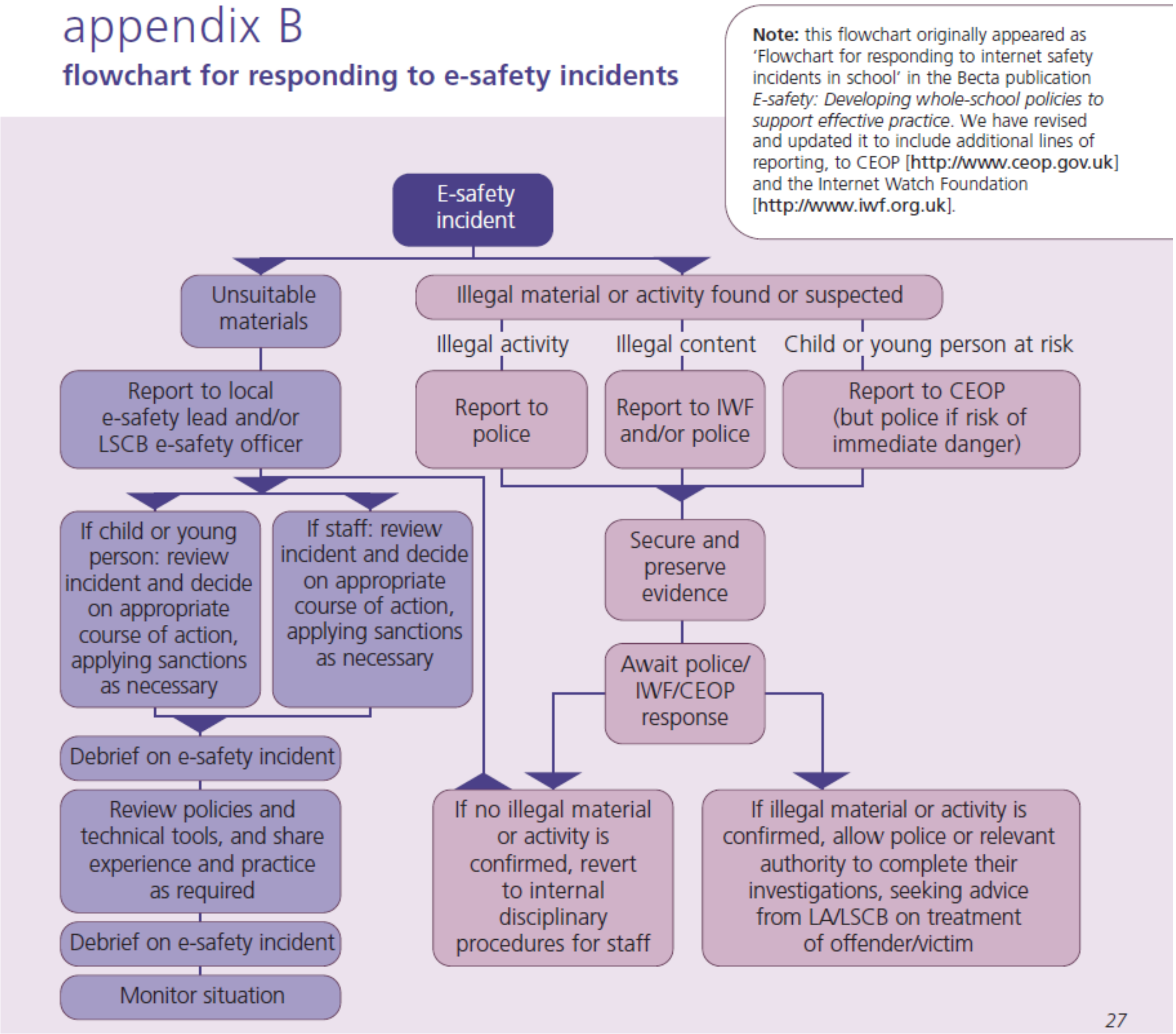
Phone ICT helpdesk and report URL if image or website.

Complete incident report.

Inform SMT

Inform parents

Apply disciplinary sanction as appropriate



appendix B

flowchart for responding to e-safety incidents

Note: this flowchart originally appeared as 'Flowchart for responding to internet safety incidents in school' in the Becta publication *E-safety: Developing whole-school policies to support effective practice*. We have revised and updated it to include additional lines of reporting, to CEOP [**http://www.ceop.gov.uk**] and the Internet Watch Foundation [**http://www.iwf.org.uk**].

E-safety incident

Unsuitable materials

Illegal material or activity found or suspected

Illegal activity

Illegal content

Child or young person at risk

Report to local e-safety lead and/or LSCB e-safety officer

Report to police

Report to IWF and/or police

Report to CEOP (but police if risk of immediate danger)

If child or young person: review incident and decide on appropriate course of action, applying sanctions as necessary

If staff: review incident and decide on appropriate course of action, applying sanctions as necessary

Secure and preserve evidence

Await police/ IWF/CEOP response

Debrief on e-safety incident

Review policies and technical tools, and share experience and practice as required

Debrief on e-safety incident

Monitor situation

If no illegal material or activity is confirmed, revert to internal disciplinary procedures for staff

If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations, seeking advice from LA/LSCB on treatment of offender/victim

Appendix C

E–Safety Audit — Primary

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e–Safety policy. Many staff could contribute to the audit including:

Designated Senior Lead, Computing Lead and Head teacher.

Has the school an e–Safety Policy that complies with Birmingham City Guidance? **Y**
Date of latest update (at least annual) – September 2015
The school e–Safety policy was agreed by governors on: 26th November 2015
The policy is available for staff at www.brookfields.bham.sch.uk
The policy is available for parents/carers at: www.brookfields.bham.sch.uk
The responsible member of the Senior Leadership Team is: Dawn Benton
The responsible member of the Governing Body is Yvonne Rogers
The Designated Senior Lead is Dawn Benton
The e–Safety Coordinator is the Computing Leader

Has ESafety training been provided for all pupils, age appropriate, and all members of staff? **Y**
Is there a clear procedure for a response to an incident of concern? **Y**
Have e–Safety materials from CEOP, Childnet and Becta been obtained? **Y**
Do all staff sign a Code of Conduct or Acceptable Use Policy on appointment? **Y**
Are all pupils aware of the e–Safety rules or Acceptable Use Policy? **Y**
Are e–Safety rules displayed in all rooms where computers are used **Y** and expressed in a form that is accessible to all pupils?
Do parents/carers sign and return an agreement that their child will **Y** comply with the School e–Safety Rules?
Are staff, pupils, parents/carers and visitors aware that network **Y** and Internet use is closely monitored and individual usage can be traced?
Has an ICT security audit been initiated by SLT, possibly using external expertise? **Y**
Is personal data collected, stored and used according to the principles **Y** of the Data Protection Act?
Is Internet access provided by an approved educational Internet service? **Y**
Has the school-level filtering been designed to reflect educational objectives **Y?**

STAFF, GOVERNORS AND VOLUNTEER ACCEPTABLE USE POLICY

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 technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion and promote creativity, promoting effective learning. They also bring opportunities for staff to be more creative and productive in their work. This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be safe and responsible users of the internet and other digital technologies;
- That school computer systems and users are protected from accident or deliberate misuse.

The school will try to ensure that staff and volunteers will have good access to computers to enhance their work and improve opportunities for learners and will, in return, expect staff and volunteers to agree to be responsible users. **This policy aims to ensure that any communication technology is used without creating unnecessary risk to users whilst supporting learning.**

Acceptable Use Policy Agreement

I understand that I must use school computer systems in a responsible way, to minimise the risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of computers and embed e-safety in my work with young people.

I agree that I will:

- Only use, move and share personal data securely
- Respect the school network security
- Implement the school's policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources
- Respect the copyright and intellectual property of others
- Only use approved email accounts
- Only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site
- Only give permission to pupils to communicate online with trusted users
- Use the computer facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues
- Not use or share my personal (home) accounts/data eg face book, with pupils
- Set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).
- Report unsuitable and/or computer misuse to the names e-safety officer
- Promote any supplied e-safety guidance appropriately.
- I know that anything I share online may be monitored

- I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I agree that I will not:

- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to pornography;
- Promote discrimination of any kind;
- Promoting violence or bullying;
- Promoting racial or religious hatred;
- Promoting illegal acts;
- Breach any Local Authority/school policies eg gambling;
- Do anything with exposes others to danger;
- Any other information which may be offensive to others;
- Forward chain letters;
- Breach copyright law;
- Use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission;
- Store images or other files off site without permission from the head teacher or their delegates representative

I will ensure that any private social networking sites, blogs, etc that I create or actively contribute to, do not compromise my professional role. I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school's management information system, private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

I accept that my use of the School and Local Authority Computing Facilities may be monitored and the outcomes of the monitoring may be used.

I have read and understand the above and agree to use the school computer systems both in and out of school and my own devices (in school, and when carrying out communications related to the school) within these guidelines.

Name: ____

Signed: ____

Date: ____

Review Date: ____

AUP GUIDANCE NOTES FOR SCHOOLS AND GOVERNORS

The policy aims to ensure that any communication technology (including computers, mobile devices and mobile phones etc) is used to supporting learning without creating unnecessary risk to users.

The governors will ensure that:

- Learners are encouraged to enjoy the safe use of digital technology to enrich their learning;
- Learners are made aware of risks and processes for safe digital use;
- All adults and learners have received the appropriate acceptable use policies and any required training;
- The school has appointed an e-safety coordinator and a named governor takes responsibility for e-safety;
- An e-safety policy has been written by the school, building on the bsb e-safety policy and becta guidance;
- The e-safety policy and its implementation will be reviewed annually;
- The school internet access is designed for educational use and will include appropriate filtering and monitoring;
- Copyright law is not breached;
- Learners are taught to evaluate digital materials appropriately;
- Parents are aware of the acceptable use policy;
- Parents will be informed that all technology usage may be subject to monitoring, including url’s and texts;
- The school will take all reasonable precautions to ensure that users access only appropriate material;
- The school will audit use of technology (using the self-review framework) to establish if the e-safety policy is adequate and appropriately implemented;
- Methods to identify, assess and minimise risks will be reviewed annually;
- Complaints of internet misuse will be dealt with by a senior member of staff.

PUPIL ACCEPTABLE USE OF ICT
AGREEMENT AND ESAFETY RULES

- I will only use Computers in school for school purposes;
- I will not tell other people my computer logon details
- I will only open/delete my own files;
- I will not bring software, CDs or computer equipment into school without permission;
- I will only use the Internet after being given permission from a teacher;
- I will make sure that all computer contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be upsetting or not allowed at school. If I accidently find anything like this, I will close the screen and tell a teacher immediately;
- I will not give out my own details such as my name, phone number or home address;
- I will be responsible for my behaviour when using computers because I know that these rules are to keep my safe;
- I know that the school may check my use of ICT and monitor the internet sites I have visited, and that my parent/carer will be contacted if a member of school staff is concerned about my e-safety.

Dear Parents/Carers

Computing, including the internet, email and mobile technologies, has become an important part of learning in schools. We expect all children to be safe and responsible when using any computers. Please read and discuss with your child the safety rules above and return this sheet signed by both you and your child. If you have any concerns or would like some explanation please contact your child's class teacher.

This Acceptable Use of Computers Agreement is a summary of our ESafety Policy which is available in full, on request at the office or can be viewed on our school website.

Pupil: I have read, understood and agreed with the Rules for Acceptable Use of Computers:

Signed: ____

Parent/Carer Consent for Internet Access: I have read and understood the school rules for Acceptable Use of Computers and give permission for my son/daughter to access the Internet in school. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet.

Signed: ____________________________________ Date: ___________________
Parent/Carer