BROWNMEAD ACADEMY

E-SAFETY POLICY

Member of Staff Responsible for Policy	K.Rosowska – Lead for ICT		
Review Committee	Curriculum Committee		
Approving Body	Full Governing Body		
Review Cycle	Bi-annually or sooner should the need arise		
Date Ratified by FGB		**Next Review**	
Review date Summary	Policy Revised or Major Re-write		
March 2015	Policy re-write		

Contents

Introduction

Roles and Responsibilities

eSafety in the Curriculum

Password Security

Data Security

Managing the Internet safely

Mobile Technologies

Managing email

Safe Use of Images

Misuse and Infringements

Equal Opportunities

Parental Involvement

Writing and Reviewing this Policy

Appendices

Acceptable Use Agreement: Staff, Governors and Visitors

Smile and Stay Safe Poster

Acceptable Use Agreement/safety rules: Pupils

Signature form

Moodle Agreement

Incident Log

Flowcharts for Managing an eSafety Incident

Current Legislation

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At **Brownmead Academy** we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of fixed and mobile internet technologies provided by the school (such as PCs, laptops, webcams, whiteboards, digital video equipment, etc.

Disclaimer: Due to the constant changes taking place within technology, this policy may not contain the most recent developments. We will however, endeavour to add any important issues to the policy on our website.

Roles and responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinator in our school is **Kasia Rosowska**. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Birmingham LA, Link2ICT, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ e-Safety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school-child agreement, and behaviour (including the anti-bullying) policy and PHSE.

e-Safety skills development for staff

- Our staff receive regular information and training on e-Safety issues in the form of staff meetings and notices.
- Details of the ongoing staff training programme can be found e-Safety co-ordinator.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart.)
- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

Managing the school eSafety messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the pupils at the start of each school year.
- E-safety posters will be prominently displayed.

e-Safety in the Curriculum

- The school provides opportunities within a range of curriculum areas to teach about e-Safety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.
- Pupils have access to activities on Internet safety on Moodle.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum in **Year 3, 4,5 & 6**

Password Security

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.
- Users are provided with a Learning Platform log-in username. From **Year 3** they are also expected to use a personal password and keep it private.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to the e-Safety co-ordinator
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically
- Due consideration should be given to security when logging into the Learning Platform to the browser/cache options (shared or private computer)

Data Security

The accessing of school data is something that the school takes very seriously. The school follows Becta guidelines (published Autumn 2008)

- Staff are aware of their responsibility when accessing school data. They must not;
- access data outside of school
- take copies of the data
- allow others to view the data
- edit the data unless specifically requested to do so by the Headteacher and/ or Governing Body.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the **Birmingham Grid for Learning** (BGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The school maintains students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, it is advised that parents check the sites and supervise the work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastucture

- Birmingham has a monitoring solution via the Birmingham Grid for Learning where web-based activity is monitored and recorded.
- School internet access is controlled through the LA's web filtering service.
- Our school has the facility for additional web filtering which is the responsibility of the e-Safety co-ordinator.
- Brownmead Academy is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the teacher and then to the e-safety co-ordinator.
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed on all school machines. This automatically updates.
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems.

- Pupils and staff are not permitted to download programs or files on school based technologies.
- If there are any issues related to viruses or anti-virus software, the e-Safety co-ordinator should be informed.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under certain circumstances the school allows a member of staff to contact a pupil or parent/ carer using their personal device.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices (including phones)

- We can provide a mobile phone in school, however staff have their own
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving emails.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated account.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform (the eSafety co-ordinator/ line manager) if they receive an offensive e-mail.
- Pupils are introduced to email as part of the ICT Scheme of Work.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.

Consent of adults who work at the school

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school's Learning Platform
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.
Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published. Only the Web Manager, (Lynne Oliver) has authority to upload to the site.

Storage of Images

- Images/ films of children are stored on the staff common
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform.
- The e-safety co-ordinator has the responsibility of deleting the images when they are no longer required, or the pupil has left the school.

Webcams and CCTV

- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- All pupils are supervised by a member of staff when video conferencing
- All pupils are supervised by a member of staff when video conferencing with end-points beyond the school.
- Approval from the Headteacher is sought prior to all video conferences within school.
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Additional points to consider:

Participants in conferences offered by 3rd party organisations may not be DBS checked.

Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

Misuse and Infringements

Complaints

Complaints relating to e-Safety should be made to the e-Safety co-ordinator or Headteacher. Incidents should be logged and the **Flowcharts for Managing an eSafety Incident** should be followed (see appendix).

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart.)
- Users are made aware of sanctions relating to the misuse or misconduct on the **Acceptable Use Agreement**

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-Safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

- Parents/ carers and pupils are actively encouraged to contribute to the school e-Safety policy by letter and by reporting unsuitable sites etc to the e-Safety co-ordinator
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to e-Safety where appropriate in the form of;
  - Website/ Learning Platform postings
  - Newsletter items

Writing and Reviewing this Policy

Staff and pupil involvement in policy creation

- Staff and pupils have been involved in making/ reviewing the e-Safety policy through staff meetings

Review Procedure

There will be an on-going opportunity for staff to discuss with the e-Safety coordinator any issue of e-Safety that concerns them.

This policy will be reviewed every (12) months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Date approved by staff: ____________

Date approved by Governors: _____________

Signed: ________________________________

Review date: ____________

Appendix

Brownmead Academy Acceptable Use Agreement/Code of Conduct: Staff, Governors and Visitors

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Kasia Rosowska school e-Safety coordinator.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences

I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
I will only use the approved, secure email system(s) for any school business.
I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
I will not install any hardware or software without seeking permission from the headteacher.
I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
I will respect copyright and intellectual property rights.
I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature
I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ……………………………………………………………………………………………………. Date ……………………

Full Name ………………………………………………………………………(printed) Job title . . . .

Appendix

Brownmead Academy Pupil Acceptable Use Agreement / e-Safety Rules

I will only use ICT in school for school purposes.
I will only use the school email address when emailing.
I will only open email attachments from people I know, or who my teacher has approved.
I will not tell other people my ICT passwords.
I will only open/delete my own files.
I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone.
I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

…and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a ‘friend’

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Appendix

Brownmead Academy

Dear Parent/ Carer

ICT including the internet, email and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mrs Rosowska.

Parent/ carer signature

We have discussed this and ……………………………………………(child name) agrees to follow the e-Safety rules and to support the safe use of ICT at Brownmead Academy.

Parent/ Carer Signature …………………………………………………….

Class …………………………………. Date ……………………………

Brownmead Academy

Dear Parent/ Carer

ICT including the internet, email and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Alyson Hackett

----

Parent/ carer signature

We have discussed this and ……………………………………………(child name) agrees to follow the eSafety rules and to support the safe use of ICT at Brownmead Academy.

Parent/ Carer Signature …………………………………………………….

Class …………………………………. Date ……………………………

Appendix

Dear Parents,

This is an agreement between the school, the children and yourselves about the use of MOODLE. **It is essential that your child's password is known only to your child in order to keep the environment safe and secure. Our administrator has full access to the site and can easily track misuse of the facilities, which will be dealt with in an appropriate manner.**

Would you and your child please read and sign the relevant sections below and return to school as soon as possible?

MOODLE Acceptable Use Agreement

Internet Rules

The school will provide each child with an individual password, which they **MUST NOT** share with **ANYONE.**

This is to ensure safety for all Brownmead children when using MOODLE.

Child

I will

- **Keep my password to myself.**
- Only use MOODLE for purposes agreed with my teacher.
- Immediately tell my teacher if I see or read anything that makes me feel uncomfortable.
- Tell my teacher straight away if I am worried about the way that someone else is using MOODLE.
- Make sure that I never tell anyone on MOODLE my address or telephone number, or those of my friends.

Child___________________________________ **Class**_______________________

I have read the 'MOODLE Rules' with my parent or guardian and I understand them.
I agree to stick to the rules when using MOODLE.

_______________________________ Child's signature.

Parent/Guardian

I have read and discussed the above stated rules with my child. I grant permission for him/her to use MOODLE. I accept responsibility for supporting the school in setting and conveying standards for my child in its use.

____________________________ Parent/guardian signature

Appendix

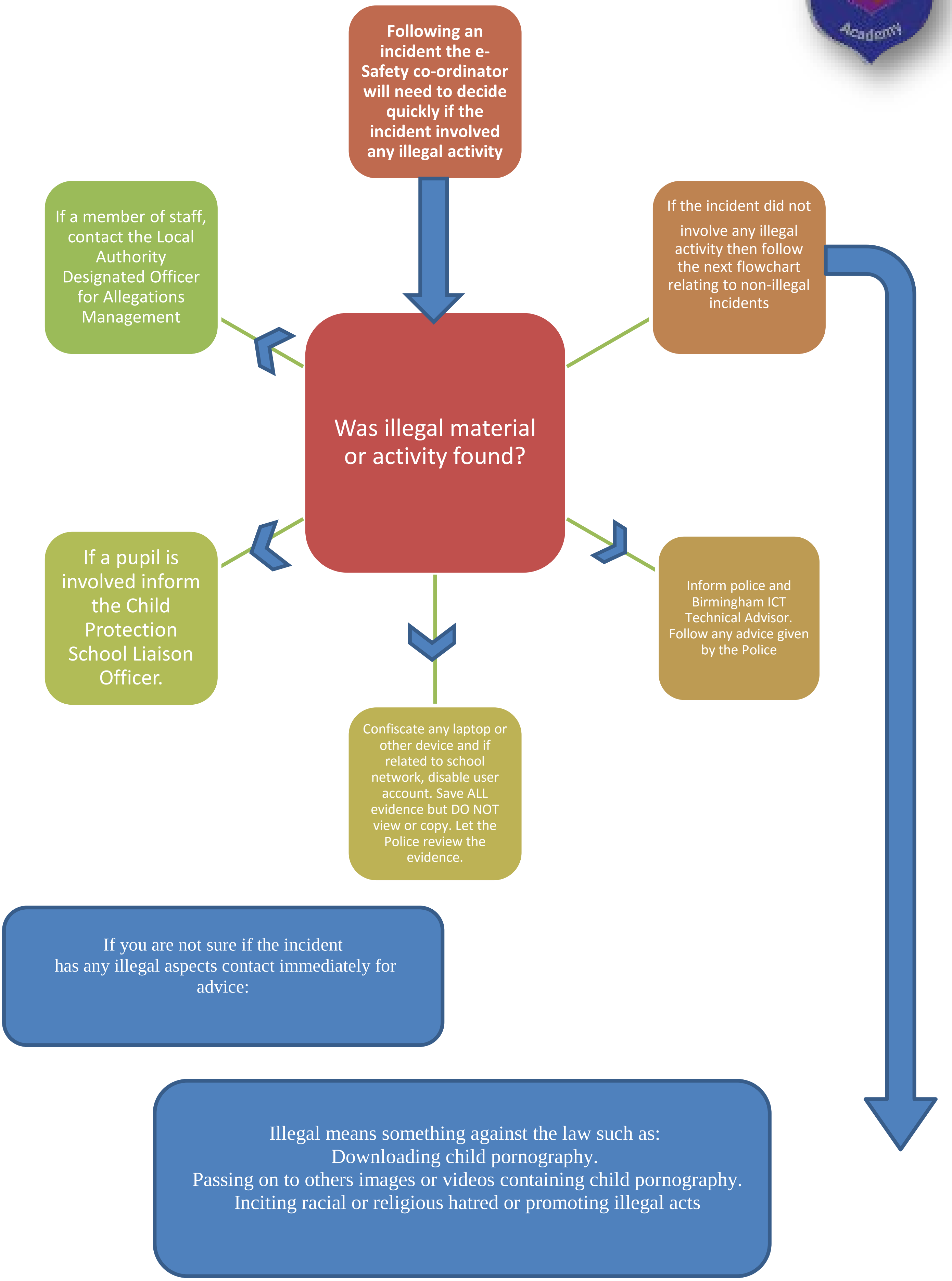
Brownmead Academy e-Safety Incident Log

Details of **ALL** e-Safety incidents to be recorded by the e-Safety co-ordinator. This incident log will be monitored by the Headteacher.

Date & Time	Name of pupil or staff	Male Or Female	Computer or Class	Details of incident (including evidence)	Actions and Reasons

Appendix

Flow chart for managing e-safety incidents



Following an incident the e-Safety co-ordinator will need to decide quickly if the incident involved any illegal activity

Was illegal material or activity found?

If a member of staff, contact the Local Authority Designated Officer for Allegations Management

If the incident did not involve any illegal activity then follow the next flowchart relating to non-illegal incidents

If a pupil is involved inform the Child Protection School Liaison Officer.

Confiscate any laptop or other device and if related to school network, disable user account. Save ALL evidence but DO NOT view or copy. Let the Police review the evidence.

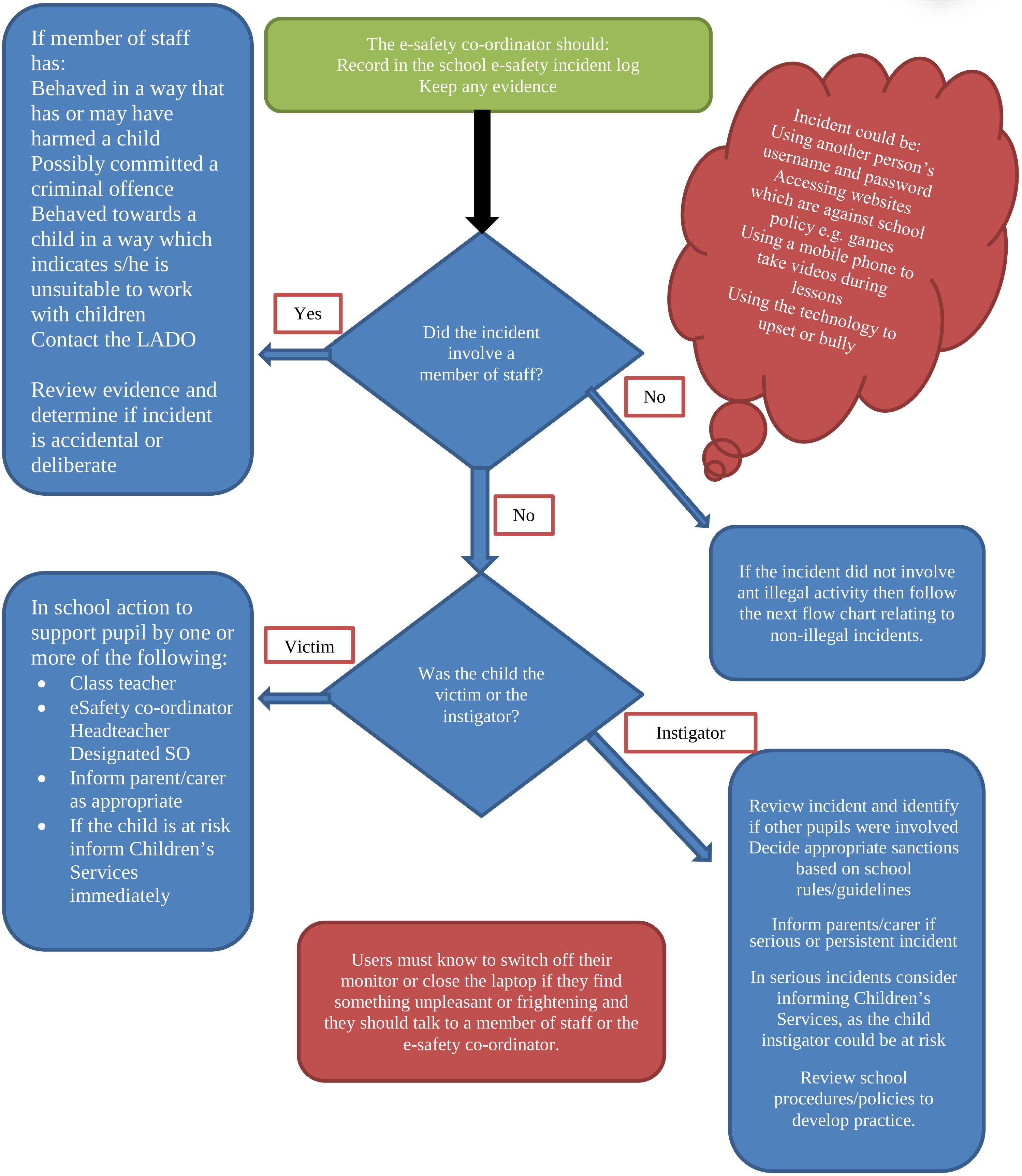
Inform police and Birmingham ICT Technical Advisor. Follow any advice given by the Police

If you are not sure if the incident has any illegal aspects contact immediately for advice:

Illegal means something against the law such as:
Downloading child pornography.
Passing on to others images or videos containing child pornography.
Inciting racial or religious hatred or promoting illegal acts

Appendix

If the incident did not involve and illegal activity follow this flow chart



The e-safety co-ordinator should:
Record in the school e-safety incident log
Keep any evidence

Did the incident involve a member of staff?

Yes

If member of staff has:
Behaved in a way that has or may have harmed a child
Possibly committed a criminal offence
Behaved towards a child in a way which indicates s/he is unsuitable to work with children
Contact the LADO

Review evidence and determine if incident is accidental or deliberate

No

Incident could be:
Using another person's username and password
Accessing websites which are against school policy e.g. games
Using a mobile phone to take videos during lessons
Using the technology to upset or bully

If the incident did not involve ant illegal activity then follow the next flow chart relating to non-illegal incidents.

No

Was the child the victim or the instigator?

Victim

In school action to support pupil by one or more of the following:

- Class teacher
- eSafety co-ordinator Headteacher Designated SO
- Inform parent/carer as appropriate
- If the child is at risk inform Children's Services immediately

Instigator

Review incident and identify if other pupils were involved
Decide appropriate sanctions based on school rules/guidelines

Inform parents/carer if serious or persistent incident

In serious incidents consider informing Children's Services, as the child instigator could be at risk

Review school procedures/policies to develop practice.

Users must know to switch off their monitor or close the laptop if they find something unpleasant or frightening and they should talk to a member of staff or the e-safety co-ordinator.

Appendix

E-Safety Rules to be displayed next to all PCs in school

Smile and Stay Safe Poster

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Appendix

Current Legislation

Acts relating to monitoring of staff email

Data Protection Act 1998
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts relating to eSafety

Racial and Religious Hatred Act 2006
It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.
For more information
www.teachernet.gov.uk

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose

of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.