Bassingbourn Village College

E-Safety and ICT Acceptable Use Policy for students

Approved/Ratified by Governors on	5th October 2017
Review cycle	3 years
Date of next review	October 2020

College Aim:

To know all our students as individuals. To provide a wide variety of opportunities and experiences through a personalised curriculum and support. To ensure rapid and sustained progress within a kind, caring and close family environment. To nurture individuals to have high aspirations, a love of learning and to become confident, responsible and independent members of society.

This policy should be read in conjunction with the Expectations for Learning and Safeguarding policies.

This policy is related to students using the school wi-fi system and the school systems. Students using their own data through their mobile phones are expected to behave in relation to the Expectation for Learning policy in regards to their use and access to social media and the internet.

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 recognize 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
- E-mail and Instant Messaging
- Chat Rooms and Social Media
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or internet capability
- Other mobile devices with internet capability

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly internet 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 Bassingbourn Village College**,** we understand the responsibility to educate our students on E-Safety 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. These issues are taught through Computing and PSHEE lessons and reiterated through tutor time, assemblies and in any lesson where students are using technology.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and our staff and students therefore have a shared responsibility to ensure that this could not be accessed by another person or organisation to cause harm or distress to an individual. Students have a responsibility to ensure that any data they share does not impact on the privacy of other members of the school community, e.g. phone numbers, addresses, social media handles.

Everybody in the school, has a duty to secure any sensitive information used day to day and should be made aware of the risks and threats and how to minimise them, including staff not directly involved in data handling. The roles and responsibilities of people affected by this policy can be found in Appendix 4.

All policies related to ICT and the student ICT Acceptable Use policy (Appendix 1)) are inclusive of both wired and wireless internet access; use of hardware provided by the school (such as PCs, laptops, tablets, webcams, voting systems, digital video equipment, etc); and hardware owned by students and staff, but brought onto school premises (such as laptops, mobile phones, smart phones, etc).

Monitoring

Authorised ICT staff may look at any ICT equipment owned or leased by the School at any time without prior notice. ICT staff may monitor, intercept, access, record and disclose e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its students without consent, to the extent permitted by law. This also includes any files saved on a student's area on the school network or sent through the school wi-fi. Use of the school wi-fi will be monitored carefully and students' access to inappropriate material will be limited whilst they are logged on through the School's network. The use of Virtual Private Networks (VPNs) or any other attempt to bypass the school's technology safeguards is prohibited when using the School's network. Students should be aware that real-time monitoring of how school hardware is being used can be done by authorized members of staff.

This monitoring may be to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT staff may, without prior notice, access the e-mail account or network area where applicable, of someone who is absent in order to deal with any work related issues retained on that account. All monitoring, surveillance or investigative activities are conducted by ICT staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded. Students need to be aware that as email accounts may be monitored, they should ensure that any messages sent comply with the ICT Acceptable Use policy and sanctions may be brought if they do not.

Breaches

A breach or suspected breach of policy by a student may result in the temporary or permanent withdrawal of access to School ICT hardware, software or services from the offending individual. A breach of policy may include, but is not limited to; the use of VPNs, sending malicious or inappropriate messages, inappropriate use of school equipment.

Any policy breach is grounds for sanctions in accordance with the Expectations for Learning policy. Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the member of the Senior Leadership Team responsible for ICT systems, currently the Principal. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the member of the Senior Leadership Team responsible for ICT systems. Incidents will be reported following the flowcharts found in Appendices 5 & 6.

Computing Facilities

Students are encouraged to make use of the college computing facilities for educational purposes. All users are expected to act responsibly and show consideration to others.

Logging on and Security

- Students are responsible for the protection of their own network logon accounts and must not divulge passwords to anyone. Anyone who feels their password has been compromised should change it immediately.
- Passwords are best when they are complex (minimum of 6 characters and including numbers, upper and lower case letters, and symbols) and are required to be changed every 6 months.
- Students are forbidden to log on as someone else, nor use a computer which has been logged on by someone else. If a device has been logged on for a long period of time but has been left unattended, students who wish to use the device may ask a member of staff to log the device out.
- All students must either log off when finished working on a device or lock the device, even for a short time.

Use of the Network and Computer facilities

It is not acceptable to:

- Play games on the school network

- Attempt to download, install, or run stand alone programmes (software and applications) on a device owned by the school.
- Attempt to introduce a virus, or malicious code.
- Attempt to bypass network and systems security, for example using a VPN.
- Attempt to gain access to another user's account.
- Attempt to gain access to an unauthorised area or system.
- Access, download, create, store or transmit material which is indecent or obscene, or material which could cause annoyance, offence or anxiety to other users, or material which infringes copyright, or material which is unlawful.
- Engage in activities which waste technical support time and resources such as unplugging cables or changing device settings
- To fix, move or alter any aspect of hardware which is the property of the school.

Use of the Internet

Access to the Internet is filtered to prevent access to inappropriate sites, and to protect the computer systems. Students should be aware that the college logs all internet use for students and for staff.

- The use of public chat rooms, social media or messaging services (such as Facebook, Twitter, Instagram, Tinder, Snapchat) is not allowed.
- Students should not copy and use material from the internet to gain unfair advantage in their studies, for example in coursework or controlled assessments. Such actions may lead to a disqualification by examination boards.
- The school has the ability to limit access to the internet during key curriculum times, e.g. controlled assessment. This will be done through the use of webzones and students are expected to follow the instructions given by staff during these times.
- Students may be expected to use separate accounts when completing controlled assessments. Students will be held accountable for these accounts and should abide by the ICT Acceptable Use Policy in the same way as they would for their standard account.
- Students should ensure that they are not breaking copyright restrictions when copying and using material from the internet.
- The use of the internet during lessons is at the discretion of the teacher.

Filtering and Prevent Strategy

The school internet is filtered by the Lightspeed Internet Filtering system. This application will restrict the access of students and staff, ensuring that they cannot access inappropriate material. The school takes safeguarding its students seriously and the system is also part of our Prevent Strategy (see Safeguarding policy for more information) to ensure that students cannot access any material that could lead to radicalization, e.g. extremist websites and videos. The Lightspeed monitoring system will alert the relevant member of senior staff of any attempt to access these materials and the appropriate actions will be taken.

Use of wifi

As a school, we encourage the use of mobile technology during times designated by the teacher. Students have the ability to log on to the school wifi network with their devices to allow them to use internet at times that computers may not be available. Students should be aware that the college logs the use of the wifi system and has the ability to identify the sites students are accessing. The wifi system has the same filters that students will experience on computers to prevent access to inappropriate sites. Students should use the wifi in accordance with the Acceptable Use Policy (Appendix 1)

- The use of public chat rooms, social media or messaging services (such as Facebook, Twitter, Instagram, Snapchat) is not allowed.
- Students are not allowed to use the school's wifi to access VPNs, which will allow them unregulated access to the internet.
- Students should not copy and use material from the Internet to gain unfair advantage in their studies, for example in coursework or controlled assessments. Such actions may lead to a disqualification by examination boards.
- Students should ensure that they are not breaking copyright restrictions when copying and using material from the internet.
- The use of mobile devices during lessons is only under the direction of the teacher.

Use of E Mail

Automated software scans all email sent to or from a school email account, and removes anything which could affect the security of the computer systems, or contain unsuitable or offensive content.

- Students are not allowed to use email during lessons, unless the teacher for that lesson has allowed its use.
- Students may only use the e mail accounts set up by the college. The use of e mail facilities such as Hotmail, Yahoo and Gmail is not permitted.
- Students should remember that email should be used appropriately and is not a messaging service for their friends.
- Students have access to the staff email addresses through their school account. These should only be used to contact staff about issues regarding a lesson, pastoral issues or for the submission of work with the agreement of the member of staff.
- Email should be used in accordance with the ICT Acceptable Use Policy (Appendix 1).

Use of Other Technologies

Technology such as smart phones, MP3 players, memory cards, USB Storage Keys and anything else that can be used to store, transmit or manipulate data should be used responsibly, and in accordance with the E-Safety and ICT Acceptable Use Policy even if not connected to the college network.

Specifically, it is an offence for mobile or smart phones or computers to be used to record and /or transmit images or messages which are obscene or which contain threats or verbal abuse. This ‘cyber bullying’ is unacceptable. Photographs, video or audio should not be taken of someone without their consent. This applies to all members of the school community, including staff, other students and visitors. Whilst it is acknowledged that it is difficult to determine whether consent has been given for a digital image, it is assumed that if the image has been taken during a lesson time, or is of a member of staff, consent has not been given. Taking and/or transmission of images/audio without consent could lead to a sanction in line with the Expectations for Learning policy.

Use of Instant Messaging

The use of Instant Messaging (IM), such as Facebook Messenger, is not permitted within the Bassingbourn Village College Network.

Social Networking

Students are not allowed to use social networking sites in school, unless under the strict guidance of a member of staff and in direct relation to the lesson content, e.g. contacting a company through Twitter to find out some information.

Students using Social networking sites outside of the school date e.g. Facebook, Twitter, Instagram, Tinder, Snapchat must NOT:

- Attempt to contact members of the staff or invite them to be friends
- Post messages/create sites which are abusive in any way towards any other members of the College community or the school itself.
- Publish or share images and videos that have been taken without consent

Students are advised not to:

- Advertise their personal information
- Leave their profiles unlocked for entire communities to read
- Reveal which social networking site they use and their social media handle on them.

Printing

All printing within the college is logged centrally for every user. Students are assigned a set amount of printer credits per month, which should only be used to print work related documents. Students found to be using the printers inappropriately may find their printer privileges restricted for a period of time.

Privacy and Personal Protection

- Students must at all times respect the privacy of others.
- Students should not supply information about themselves, or any other member of the College Community, on websites, within email, social media or instant messaging.
- Students must not attempt to arrange meetings with anyone met via websites, email, social media or instant messaging
- Students should realize that the college has a right to access personal folders on the Network. Privacy will be respected unless there is reason to think that someone is not following the E-Safety and ICT Acceptable Use Policy in which case they will be subject to disciplinary procedures.

E-safety

Students will be taught about e-safety through PSHEE, assemblies and Computing lessons. Guidance will be given to ensure that the students are aware of, amongst other things; how to keep safe online, what to do if they find themselves in a situation they are uncomfortable with, how to be a responsible member of the internet community and how to ensure that internet searches produce appropriate results. E-safety will be re-iterated in any lessons that involve the use of computers or the internet.

Students will also be regularly reminded about their social media presence and given guidance about how to ensure privacy settings are set appropriately and reminded that their social media footprint will be a long-standing legacy that may be viewed by future employers and sixth form administrations. Students should ensure that their social media posts comply with the E-Safety and ICT Acceptable Use Policy and do not contain any offensive or inappropriate language or anything directed at other members of the school community and the school itself.

Confirmation of agreement

All students will be introduced to this policy in either Computing lessons or tutor time and must confirm that they agree to abide by all aspects of this policy each time they access the College Network. This agreement will be formalized through the signing of the Acceptable Use Policy (Appendix 1). Students who do not sign the agreement will find their ability to use school devices is limited.

Appendix 1 Bassingbourn Village College ICT Acceptable Use Agreement (Student)

**Acceptable use of computers and personal devices at Bassingbourn Village College
A Policy and Guidance document**

Internet and wifi

1. I will not visit websites that contain unsuitable material. If I am unsure if a site is suitable, I will ask a member of staff.
2. I will not attempt to access VPNs through the school wifi.
3. During lessons and extra-curricular clubs I will only use the Internet as directed by staff. If I want to use the Internet for any other purpose, I will ask permission first.
4. I will not take information from the Internet and pass it off as my own work.
5. Whilst in school, the Internet is for educational use. I will not use it via school wifi or my own data to access social networking sites like Facebook, Snapchat or Twitter.

Email, social media and on-line communication

1. To keep myself safe I will not give out personal information in an email or on the Internet.
2. I will remember that email that is sent out using my college email address represents the school.
3. I will be responsible in my use of email and social media.
4. I will not include any material that is inappropriate in an email or on social media.
5. I will not publish or share any images that were taken without consent.
6. I will report any misuse of email or social media. I will forward any email I am concerned about to abuse@bassingbournvc.net

Network

1. I will not attempt to gain unauthorized access to any part of the Bassingbourn Village College network or to any other computer system found via the Internet.
2. I will not attempt to log on using another person's username and password with or without their permission.
3. I will not attempt to access, change, move or delete another person's files.
4. I will not try to alter the settings on any BVC computer.
5. I will only copy pictures or text into my area on the network.
6. I will not download any other type of file (for example software, games, screen savers, any executable file)
7. I understand that Bassingbourn Village College retains the right to monitor all areas of the College network including my personal file space to ensure adherence to this policy.

Language and bullying

1. I will not use offensive or threatening language in my emails, or in any other communication via the Internet or social media.
2. I understand that normal school policies, expectations and sanctions apply to behaviour and bullying in any form of electronic communication.

Student

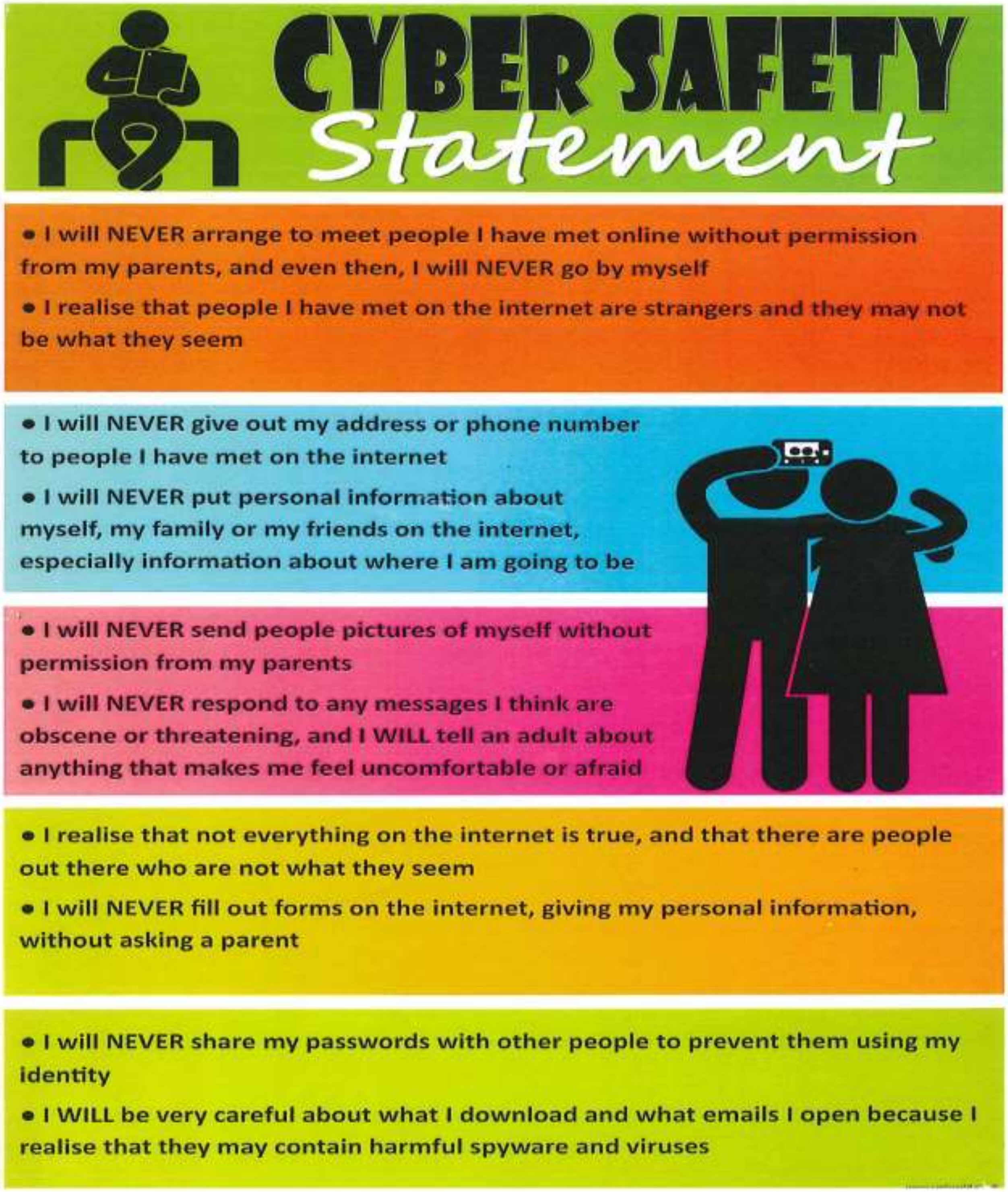
I understand that my parents will be informed if I misuse the internet or social media and that this policy extends to the BVC Expectations for Learning Policy. I have read this policy and agree to follow it.

Student signature ____________________________Tutor Grp ____________

Parent/Guardian ____

The Acceptable Use Agreement for staff and governors can be found in the Personnel handbook.

Appendix 2 – Cybersafety poster – displayed in student areas



CYBER SAFETY Statement

- I will NEVER arrange to meet people I have met online without permission from my parents, and even then, I will NEVER go by myself
- I realise that people I have met on the internet are strangers and they may not be what they seem

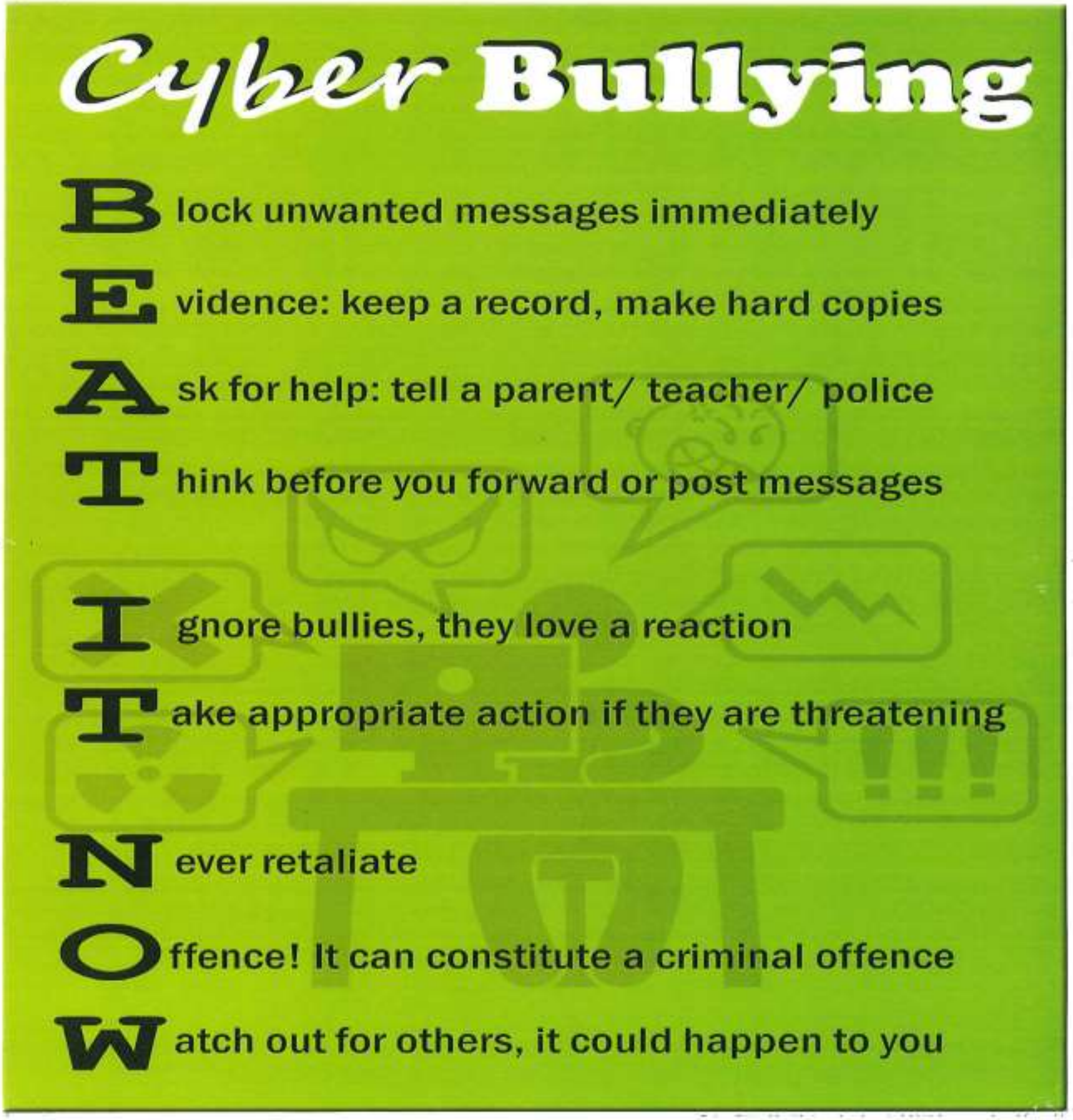
- I will NEVER give out my address or phone number to people I have met on the internet
- I will NEVER put personal information about myself, my family or my friends on the internet, especially information about where I am going to be

- I will NEVER send people pictures of myself without permission from my parents
- I will NEVER respond to any messages I think are obscene or threatening, and I WILL tell an adult about anything that makes me feel uncomfortable or afraid

- I realise that not everything on the internet is true, and that there are people out there who are not what they seem
- I will NEVER fill out forms on the internet, giving my personal information, without asking a parent

- I will NEVER share my passwords with other people to prevent them using my identity
- I WILL be very careful about what I download and what emails I open because I realise that they may contain harmful spyware and viruses

Appendix 3 – Cyberbullying poster – displayed in student areas



Cyber Bullying

Block unwanted messages immediately

Evidence: keep a record, make hard copies

Ask for help: tell a parent/ teacher/ police

Think before you forward or post messages

Ignore bullies, they love a reaction

Take appropriate action if they are threatening

Never retaliate

Offence! It can constitute a criminal offence

Watch out for others, it could happen to you

<u>Appendix 4 – Roles & Responsibilities</u>

Principal

Reporting to the governing body, the Principal has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-Safety Officer (or more than one), as indicated below.

The Principal will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated e-Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

Person with e-Safety responsibility (Vickey Poulter)

The member of staff with e-Safety responsibility will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Principal.
- Advise the Principal, governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make him/herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Principal to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any e-safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the member of staff responsible for e-safety and Principal.
    - Passwords are applied correctly to all users regardless of age

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Principal.
- Any e-safety incident is reported to the member of staff responsible for e-Safety (and an e-Safety Incident report is made), or in his/her absence to the Principal.
- The reporting flowcharts (Appendices 5 & 6) contained within this e-safety policy are fully understood.

All Students

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the Expectations for Learning policy.

e-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

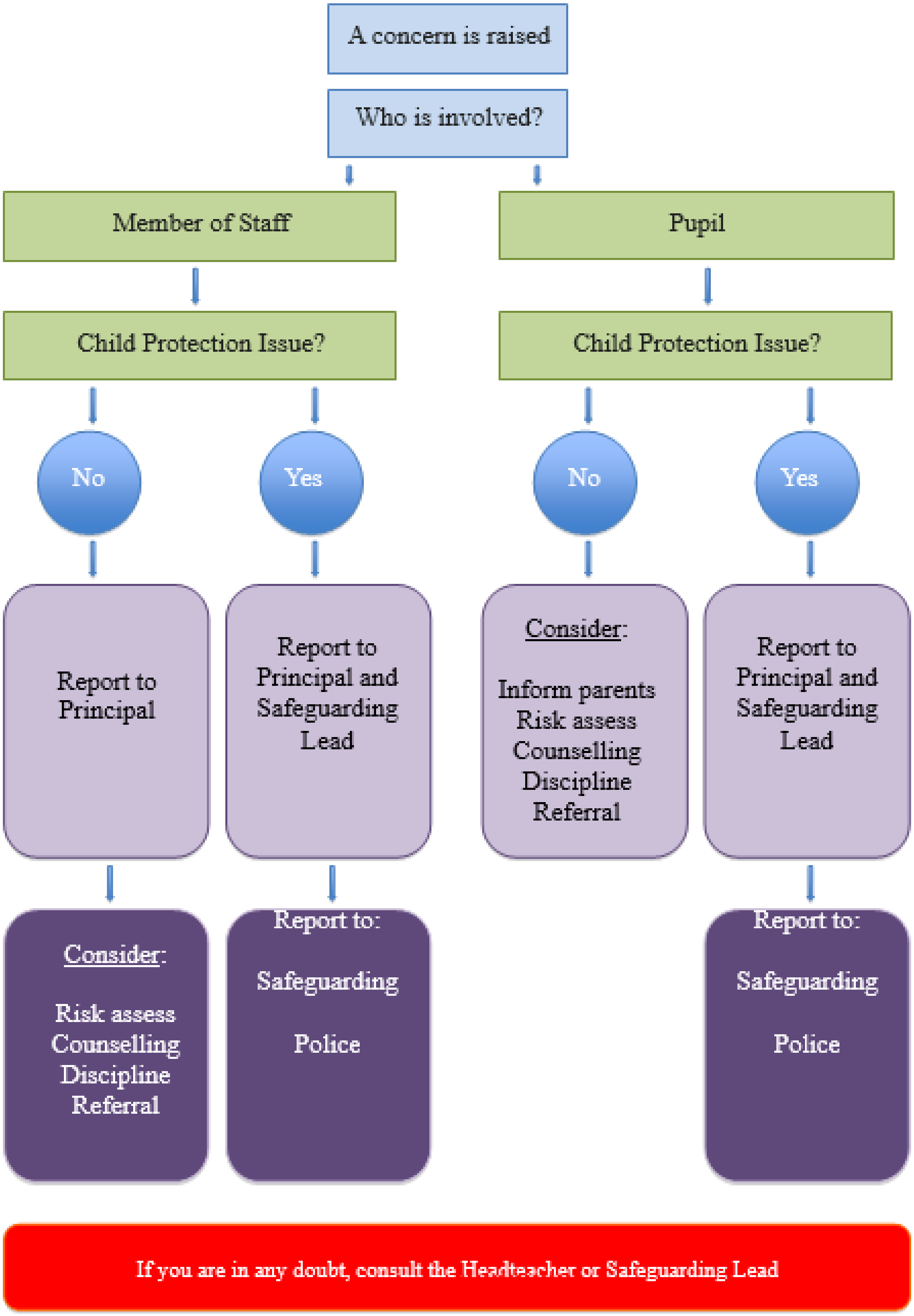
Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents information evenings, parentmail and school newsletters the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

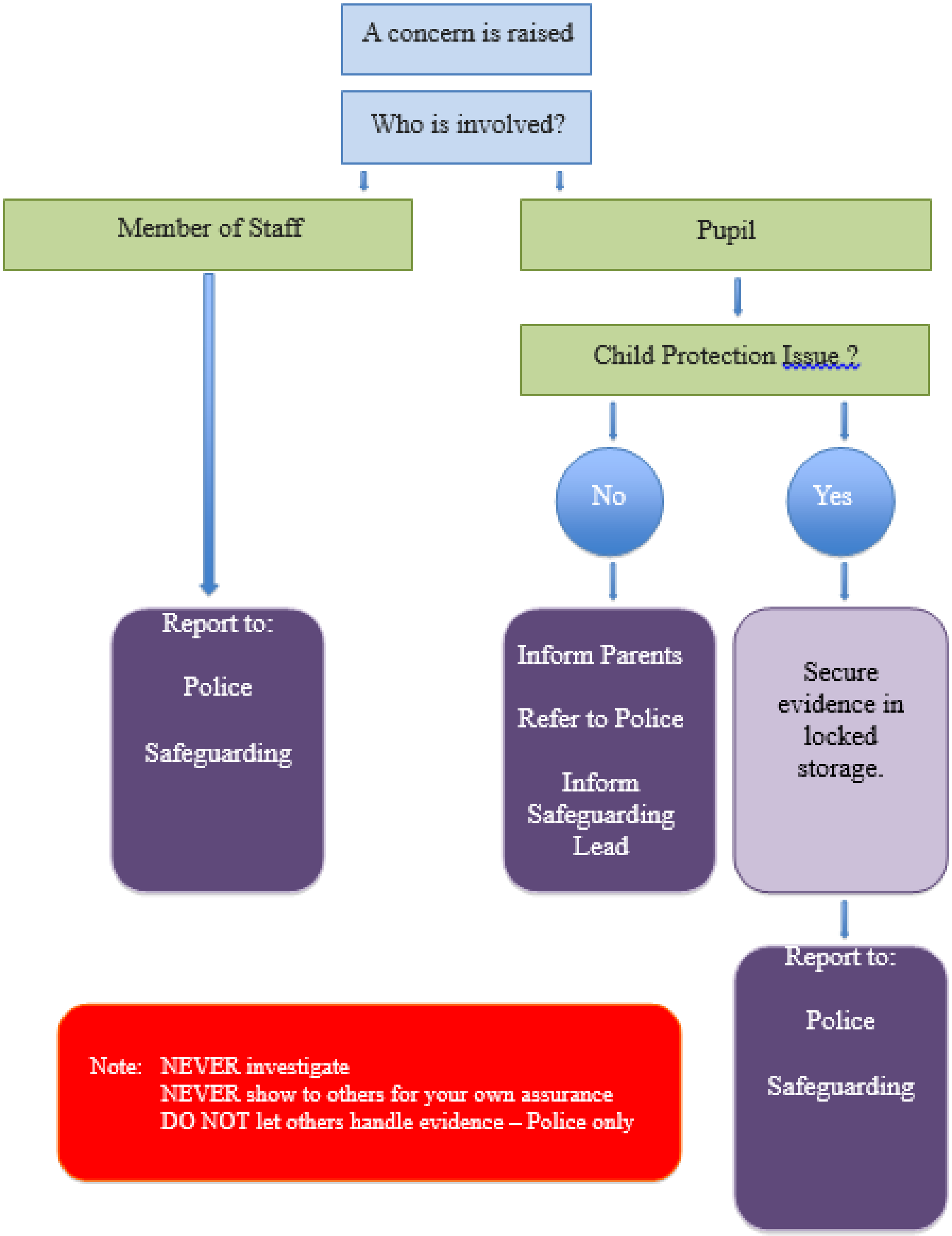
<u>Appendix 5 – Inappropriate Activity</u>

Inappropriate Activity Flowchart



Appendix 6 – Illegal Activity

Illegal Activity Flowchart



Note: NEVER investigate
NEVER show to others for your own assurance
DO NOT let others handle evidence – Police only