ACCEPTABLE AND RESPONSIBLE USE INTERNET POLICY INCLUDING CYBER BULLYING

- *This page left intentionally blank* -

- Acceptable and Responsible Internet Policy
- including Cyber Bullying

Rationale

The Internet is an open communication channel, available to all. Applications such as the Web, email and chat all transmit information over the wires and fibers of the Internet to many locations in the world at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features make it a valuable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition there is information on weapons, crime and racism that would be more restricted elsewhere. Sadly, email and chat communication can provide opportunities for adults to make contact with children for inappropriate reasons. At Albany Village Primary School, in line with policies that protect pupils from other dangers, we will provide pupils with as safe an Internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.

We will protect our school from possible legal challenge wherever possible. The legal system continues to struggle with the application of existing decency laws to computer technology. It is clearly an offence to hold images of child pornography on computers and to use Internet communication to “groom” children. However, the possession of other obscene or offensive material is not clearly defined. The Computer Misuse Act 1990 makes it a criminal offence to “cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer”. At Albany Village Primary School we will make it clear to users that the use of school equipment to view or transmit inappropriate material is “unauthorised”. However, we are aware that a disclaimer is not sufficient to protect a school from a claim of personal injury and we will ensure that all reasonable and appropriate steps have been taken to protect pupils. Staff are aware of many risks of Internet use and have had opportunities for detailed discussion. Advice and training has been provided to staff from advisors and safeguarding/child protection leads. A Social Media Policy has been developed and introduced to staff September 2016.

Why is Internet use important?

The purpose of Internet access in schools 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 mature and responsible approach to its use. The Internet is an essential element in 21st century life for education, business and social interaction. Our school has a duty to provide pupils with quality Internet access as part of their learning experience. Robust filtering software is in place as well as FutureCloud monitoring software to further protect children from radicalisation.

How does the Internet benefit education?

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and galleries.
- Inclusion in Government initiatives.
- Education and cultural exchange between pupils worldwide.
- Immediate access to up to the minute news and current events.
- Cultural, vocational, social and leisure use in libraries, clubs and at home.
- The opportunity for staff and pupils to discuss with experts in a variety of fields.
- Staff professional development through access to national developments, educational resources and good curriculum practice.
- Communication with support agencies, professional associations and colleagues.
- Improved access to technical support including remote management of networks.
- Exchange of curriculum and administrative data with LA and DfE.

Scope

This policy applies to all school equipment at any time including any mobile devices signed out by staff for use at home. Visitors should seek the Head Teacher's permission before bringing their own equipment onto the premises. Visitors are advised of this requirement when initially contacting the school or when signing in procedures are carried out.

Risk Assessment

As with a number of other media sources, such as magazines, books and videos, the Internet contains material unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material by using a robust filtering system together with FutureCloud monitoring software. Children will not be allowed Internet access without the presence or guidance of an adult member of staff. Staff supervision is paramount in taking all reasonable precautions to ensure only appropriate material is accessed.

However, even with adult supervision or guidance, it is impossible to guarantee that particular types of material will never appear on a computer terminal or station. This is due to the international scale and linked nature of material on the Internet. The school cannot accept liability for inadvertent access to material accessed or to the consequences of such 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 annually. The Head Teacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

Policy Decisions

- No pupil will use the ICT suite without adult supervision.
- Pupils must have permission to use the Internet.
- Pupils may work independently when directed to a website which has already been vetted by the teacher.

- Free searching, using general search engines e.g. Google, is forbidden to pupils unless they work closely with and under the direct supervision of a teacher. No pupil will be allowed to independently carry out a free search.
- Free searching for pupils can be undertaken if pupils are using recommended children's search engines such as yahooligans or ask kids; however pupils will still work with supervision from the teacher.
- Only an adult or children under supervision will do the downloading of files or images.
- Children will not use or be issued with individual e-mail accounts. Staff in school must only use approved email accounts set up on the school system.
- Pupils who use email and social media accounts outside of school will be reminded that they must not reveal personal details of themselves (home address, telephone number) or personal details of others in emails, social media or online chat apps and that they must not arrange to meet anyone.
- Pupils are advised to immediately tell staff if they receive any offensive material or inappropriate communication or anything else that causes them upset.
- E-mail sent by staff to external organisations must be adhere to school policy in the same way as a letter written on school headed paper.

Social networking and personal publishing

- The school does not permit access to social networking sites
- Newsgroups are also blocked
- Pupils are told never to give out personal details which may identify them
- Pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Authorising Internet Access

The school has in place Internet access based on educational or professional development needs. Any other use of the internet may be allowed but must be agreed to by the School Management Team before use. Under no circumstances will free games access be allowed.

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff or pupil may leave or a pupil's access be withdrawn. There will be a separate access for pupils and supply staff.

In our school Internet access is granted to the whole class based on a lesson need that corresponds to the ICT or cross curricular Schemes of Work. Pupils, if required, will be allowed supervised use of the Internet for research or reference outside of class time (e.g. break times or after school clubs). All pupils are given a comprehensive introduction and additional reminders throughout the year to ensure responsible use of the Internet. They must also individually agree to abide by the Cyber Safe Agreement. (Appendix 1) by signing themselves and countersigned by the Parent/Carer.

All staff/students/volunteers are expected to comply fully with the school's Acceptable and Responsible Internet Policy. Failure to do so may be a disciplinary offence.

Maintaining a Secure Computer System

- The school's ICT provider filters the school's internal network via specific software
- Virus protection software is installed and is updated regularly
- Security strategies will be discussed with the school's ICT provider as appropriate. The use of external media ie: cd-roms, SD cards or memory stick by children is not permitted
- Staff are issued with encrypted memory stick for school use only and are not permitted to use their own personal media.
- The ICT Technician, together with the E-Safety Team, will ensure the school's system capacity is reviewed regularly.
- Monitoring software is installed to safe guard staff and pupils which is checked by the ICT Technician
- Children can save their work within an allocated area on the network which is totally secure and separate from school files.

Data Protection

Staff must only use encrypted memory sticks.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Procedures for Reporting Inappropriate use of I.T.

Responsibility for handling incidents will be delegated to the E-Safety Team in consultation with the Head Teacher:

- User reports immediately, but discreetly, to the supervising adult.
- The supervising adult will turn off the monitor but not the base unit.
- A member of the E-Safety team will be informed.
- The ICT Technician and E-Safety Team member will privately review the nature of the material and will log the terminal number/location, the date, time and nature of material found, who found it and the user login if appropriate.
- This information is forwarded to the Head Teacher who will accept responsibility, or allocate responsibility to the Deputy Head, for dealing with the incident.

Depending on the seriousness of the incident:

I. Pupils and parents will be informed of the incident and complaints procedure.
II. Parents and pupils may need to work in partnership with staff to resolve an issue.
III. There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies.
IV. A pupil may have Internet or computer access suspended.
V. If unsuitable sites are discovered the URL (address) and content will be reported to the school's ICT provider as Internet service provider, CEOPS and the Police.

Any complaint about staff misuse must be referred to the Head Teacher who will follow protocol and liaise with appropriate agencies ie: Designated Officer, Police, HR.

Staff Internet Use

Staff must only access computers using their own accounts. Staff use of the Internet is restricted to professional use only. The Internet on school computers should not be used for any political purposes, personal gain or social use e.g. personal emails, booking holidays, private financial matters or social networking.

Where school mobile devices are used outside of school staff are required to follow the policy with regard to the use of the Internet outside of school premises. All staff are required to sign and adhere to the policy.

- Random checks on Internet history will be undertaken and logs maintained.
- Inappropriate use of the Internet will be subject to disciplinary action.
- Staff must ensure they log off their computer when left unattended.
- Staff must ensure that pupils or other members of staff are not allowed access to their computer/laptop when they are logged on to the system with their personal teacher username/password.

Keeping staff and pupils aware of their Conditions of Use

All staff and adults working in school will be given a copy of the 'Acceptable and Responsible Use of Internet Policy' and its importance explained. Users will be required to sign an agreement indicating their acceptance of school policy before being issued with a logon account. If they feel unprepared for Internet use then a member of the E-Safety Team or the ICT Technician will support them. (Appendix 2)

A Staying Safe Guide will be displayed near all computer systems (see Appendix 3).

Children will be reminded at the beginning of every academic year of the rules of acceptable use of IT and issued with the Staying Safe Guide and Cyber Safe Agreement.

Parental Support

The school aims to provide parents with as much support and information as possible. We do this by firstly drawing parents' attention to the school's Acceptable and Responsible Internet Use Policy as well as providing information in newsletters, the school brochure and on our website. The school provides parents with the following information to support them with keeping their children safe when online at home:-

- Invite to Annual E-Safety conference : e-safety information pack
- E-Safety Leaflet – be a good digital parent
- Safeguarding First : Social Media & Applications Guidance for Parents
- E-Safety page on website dedicated to staying safe on line
- Links to appropriate websites and organisations who provide valuable information ie: CEOPS, Think U Know

Review

The Governing Body will review this policy annually. The Governors may, however, review the policy earlier if the Government introduces new legislation, or if the Governing Body receives recommendations on how the policy may be improved.

Equality Act

The Equality Act 2010 introduced a duty to promote equality of opportunities.

As a school we have a strong belief in inclusion. We feel that it is the responsibility of the whole school community to implement an equality scheme that promotes the inclusive ethos of our school.

Our policies have been written to ensure that inclusion is promoted.

Appendix 1

Having access to technology is a wonderful thing and being online is part of that.
Following this agreement will help you to make sure that you have fun and stay safe wherever you use technology.
Read through it with your parent and make sure you both understand before signing it below.

I will be a good communicator
by using good manners at all times and never being rude
or nasty to to others in my emails, texts and online conversations.

I will only accept good communication
by expecting good manners from people who email, text or have online conversations with me.
If anyone says or does anything to upset me
I will keep the messages and show them to a trusted adult.

I will be careful what I post
I'll stop and think about the consequences before I post something online.
I will never post or forward information, photos or videos that could cause embarrassment or put me or anyone else at risk.

I will be careful who I have as an online friend
by accepting people that I really know and only sharing my profiles with friends

I will be careful what I share
by keeping my personal information private. I will never share my, or anyone else's, full name, address, passwords, school name, email address, current location or phone numbers with anyone online.

I will be careful who I meet
I won't meet up with anyone
I talk to online unless my parent or carer
says its ok and they come with me.

I will listen to my feelings
and tell a trusted adult if anything I see or hear online
makes me feel sad, scared or confused.

I will make sensible choices wherever I am
At school by only accessing sites that help me to learn.
At home by choosing sites and games
that are meant for young people my age.

I agree to follow the Cyber Safe agreement

I agree to support ..... (young person) to follow the Cyber Safe agreement

..... Signature of young person

..... Signature of Parent/Carer

Appendix 2

Staff : Responsible Internet Use Statement

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties – the pupils' the staff and the school. The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff requesting Internet access should sign a copy of this Acceptable Use Statement and return it to the ICT leader or Headteacher for approval.

- Access should only be made via the authorised account and password, which should not be made available to any other person
- Activity that threatens the integrity of the school ICT system or activity that attacks or corrupts other systems is forbidden
- Users are responsible for all email sent and for contacts made that may result in an email being received
- Posting anonymous messages and forwarding chain letters is forbidden
- Copyright of materials must be respected
- All Internet activity should be appropriate for staff professional activity or pupils' education
- The same professional levels of language and content should be applied as for letters or other media, particularly as email is often forwarded or may be sent inadvertently to the wrong person
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Users must only access those sites and materials relevant to their work in school
- Users must log off when they leave the room
- Users will be aware when they are accessing inappropriate material and should expect to have their permission to use the system removed.
- Staff should not give their password or email address to pupils

This applies to both hardware in school and any staff laptops or additional mobile devices signed out for use at home.

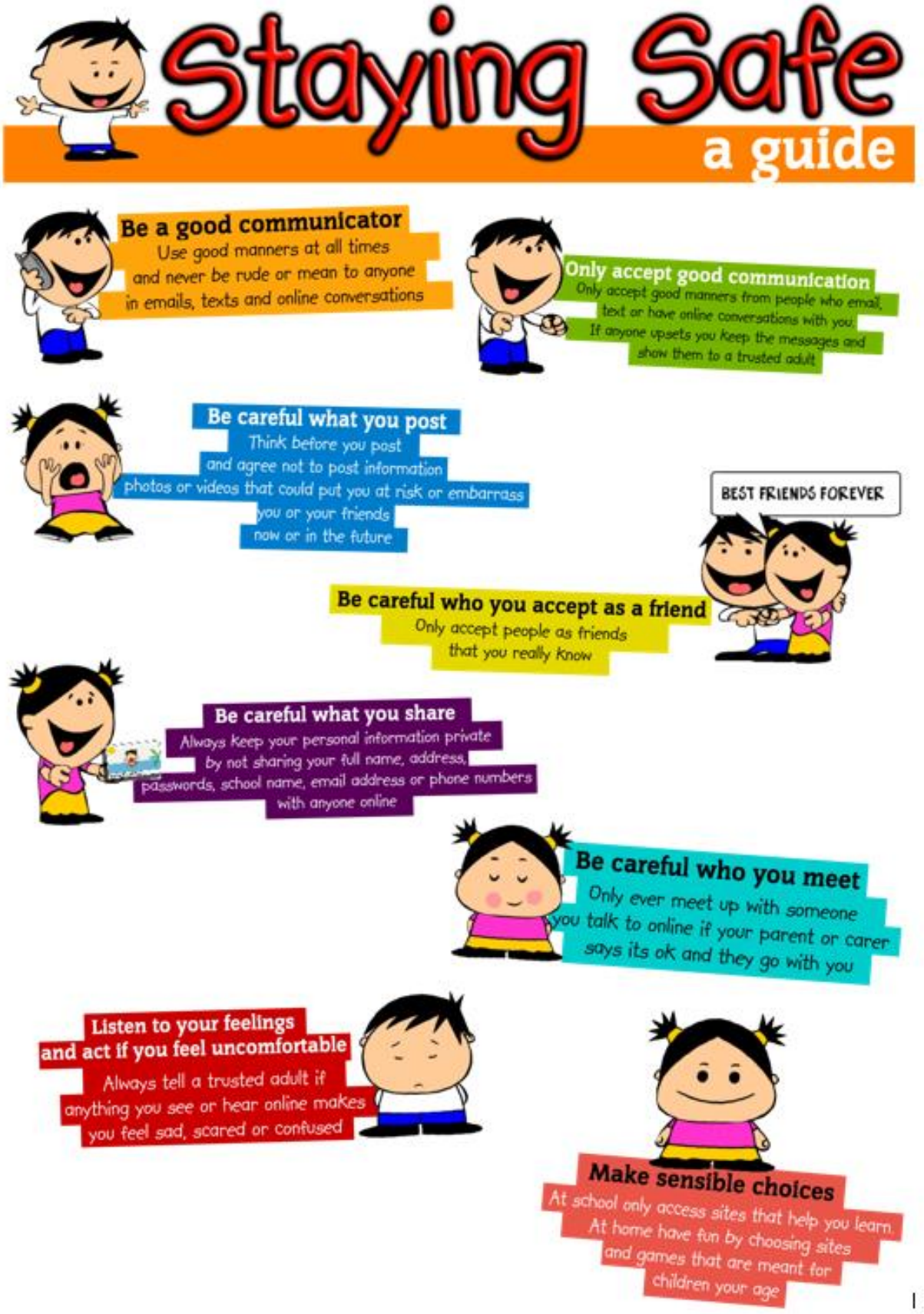
Any material breach of this will result in disciplinary action

Full Name _____ Post _____

Signed _____ Date_____

Access Approved _____ Date _____

Appendix 3


Staying Safe
a guide
Be a good communicator
Use good manners at all times and never be rude or mean to anyone in emails, texts and online conversations
Only accept good communication
Only accept good manners from people who email, text or have online conversations with you. If anyone upsets you keep the messages and show them to a trusted adult
Be careful what you post
Think before you post and agree not to post information photos or videos that could put you at risk or embarrass you or your friends now or in the future
BEST FRIENDS FOREVER
Be careful who you accept as a friend
Only accept people as friends that you really know
Be careful what you share
Always keep your personal information private by not sharing your full name, address, passwords, school name, email address or phone numbers with anyone online
Be careful who you meet
Only ever meet up with someone you talk to online if your parent or carer says its ok and they go with you
Listen to your feelings and act if you feel uncomfortable
Always tell a trusted adult if anything you see or hear online makes you feel sad, scared or confused
Make sensible choices
At school only access sites that help you learn. At home have fun by choosing sites and games that are meant for children your age

Cyber-bullying

This school believes that all people in our community have the right to teach and learn in a supportive, caring and safe environment without fear of being bullied. We believe that every individual in school has a duty to report an incident of bullying whether it happens to themselves or to another person.

WHAT IS CYBER-BULLYING?
There are many types of cyber-bullying. Although there may be some of which we are unaware, here are the more common.

1. **Text messages** —that are threatening or cause discomfort - also included here is "Bluejacking" (the sending of anonymous text messages over short distances using "Bluetooth" wireless technology)

2. **Picture/video-clips** via mobile phone cameras - images sent to others to make the victim feel threatened or embarrassed.

3. **Mobile phone calls** — silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible.

4. **Emails** — threatening or bullying emails, often sent using a pseudonym or somebody else's name.

5. **Chatroom bullying** — menacing or upsetting responses to children or young people when they are in web-based Chatroom.

6. **Instant messaging** (IM) — unpleasant messages sent while children conduct real-time conversations online using MSM (Microsoft Messenger), WhatsApp, SnapChat, Instagram Chat – although there are others.

7. **Bullying via websites** — use of defamatory blogs (web logs), personal websites and online personal "own web space" sites such as Bebo (which works by signing on in one's school, therefore making it easy to find a victim) and MySpace – although there are others.

At Albany Village Primary School, we take this bullying as seriously as all other types of bullying and, therefore, will deal with each situation individually. An episode may result in a simple verbal warning. It might result in a parental discussion. Clearly, more serious cases will result in further sanctions.

Technology allows the user to bully anonymously or from an unknown location, 24 hours a day, 7 days a week. Cyber-bullying leaves no physical scars so it is, perhaps, less evident to a parent or teacher, but it is highly intrusive and the hurt it causes can be very severe.
Young people are particularly adept at adapting to new technology, an area that can seem a closed world to adults. For example, the numerous acronyms used by young people in chat rooms and in text messages (POS - Parents Over Shoulder, TUL – Tell You Later) make it difficult for adults to recognise potential threats.

At Albany Village Primary School, pupils are taught how to:

- Understand how to use these technologies safely and know about the risks and consequences of misusing them.
- Know what to do if they or someone they know are being cyber bullied.
- Report any problems with cyber bullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it.

Albany Village Primary School has:

1. An Acceptable Use Police (AUP) that includes clear statements about e communications

2. Information for parents on: E-communication standards and practices in schools, what to do if problems arise, what's being taught in the curriculum.

3. Support for parents and pupils if cyber bullying occurs by: assessing the harm caused, identifying those involved, taking steps to repair harm and to prevent recurrence

<u>Guidance for pupils</u>

If you're being bullied by phone or the Internet

- Remember, bullying is never your fault. It can be stopped and it can usually be traced.
- Don't ignore the bullying. Tell someone you trust, such as a teacher or parent, or call an advice line.
- Try to keep calm. If you are frightened, try to show it as little as possible. Don't get angry, it will only make the person bullying you more likely to continue.
- Don't give out your personal details online - if you're in a Chatroom, watch what you say about where you live, the school you go to, your email address etc. All these things can help someone who wants to harm you build up a picture about you.

- Keep and save any bullying emails, text messages or images. Then you can show them to a parent or teacher as evidence.
- If you can, make a note of the time and date bullying messages or images were sent, and note any details about the sender.
- There's plenty of online advice on how to react to cyber bullying. For example, **www.kidscape.org** and **www.wiredsafety.org** have some useful tips:

Text/video messaging

- You can easily stop receiving text messages for a while by turning off incoming messages for a couple of days. This might stop the person texting you by making them believe you've changed your phone number. If the bullying persists, you can change your phone number. Ask your mobile service provider.
- Don't reply to abusive or worrying text or video messages. Your mobile service provider will have a number for you to ring or text to report phone bullying. Visit their website for details.
- Don't delete messages from cyber bullies. You don't have to read them, but you should keep them as evidence. Text harassment is a crime.
- If the calls are simply annoying, tell a teacher, parent or carer. If they are threatening or malicious and they persist, report them to the police, taking with you all the messages you've received.

Phone calls

- If you get an abusive or silent phone call, don't hang up immediately. Instead, put the phone down and walk away for a few minutes. Then hang up or turn your phone off. Once they realise they can't get you rattled, callers usually get bored and stop bothering you.
- Always tell someone else: a teacher, youth worker, parent, or carer. Get them to support you and monitor what's going on.
- Don't give out personal details such as your phone number to just anyone and never leave your phone lying around.
- When you answer your phone, just say 'hello', not your name. If they ask you to confirm your phone number, ask what number they want and then tell them if they've got the right number or not.
- You can use your voicemail to vet your calls. A lot of mobiles display the caller's number. See if you recognise it. If you don't, let it divert to voicemail instead of answering it.
- Don't leave your name on your voicemail greeting. You could get an adult to record your greeting. Their voice might stop the caller ringing again. Almost all calls nowadays can be traced. If the problem continues, think about changing your phone number. If you receive calls that scare or trouble you, make a note of the times and dates and report them to the police. If your mobile can record calls, take the recording too.

Emails

- Never reply to unpleasant or unwanted emails ('flames') — the sender wants a response, so don't give them that satisfaction.
- Keep the emails as evidence. And tell an adult about them.
- Ask an adult to contact the sender's Internet Service Provider (ISP) by writing abuse@ and then the host, e.g. **abuse@hotmail.com**
- Never reply to someone you don't know, even if there's an option to 'unsubscribe'. Replying simply confirms your email address as a real one.

Web bullying

- If the bullying is on a website (e.g. Bebo) tell a teacher or parent, just as you would if the bullying were face-to-face – even if you don't actually know the bully's identity.
- Serious bullying should be reported to the police - for example threats of a physical or sexual nature. Your parent or teacher will help you do this.

Chat rooms and instant messaging

- Never give out your name, address, phone number, school name or password online. It's a good idea to use a nickname. And don't give out photos of yourself.
- Don't accept emails or open files from people you don't know. Remember it might not just be people your own age in a chat room.
- Stick to public areas in chat rooms and get out if you feel uncomfortable.
- Tell your parents or carers if you feel uncomfortable or worried about anything that happens in a chat room.
- Think carefully about what you write; don't leave yourself open to bullying.
- Don't ever give out passwords to your mobile or email account.

Three steps to stay out of harm's way

1. Respect other people - online and off. Don't spread rumours about people or share their secrets, including their phone numbers and passwords.

2. If someone insults you online or by phone, stay calm – and ignore them.

3. 'Do as you would be done by.' Think how you would feel if you were bullied. You're responsible for your own behaviour – make sure you don't distress other people or cause them to be bullied by someone else.

<u>The law is on your side</u>

The **Protection from Harassment Act**, the **Malicious Communications Act 1988** and Section 43 of the **Telecommunications Act** may be used to combat Cyber bullying. People may be fined or sent to prison for up to six months.

Additional information

"Bluejacking" (the sending of anonymous text messages over short distances using "Bluetooth" wireless technology)

Picture/video-clips via mobile phone cameras - images sent to others to make the victim feel threatened or embarrassed.

Mobile phone calls — silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible.

Emails — threatening or bullying emails, often sent using a pseudonym or somebody else's name.

Chatroom bullying — menacing or upsetting responses to children or young people when they are in web-based Chatroom.

Instant messaging (IM) — unpleasant messages sent while children conduct real-time conversations online using MSM (Microsoft Messenger) or Yahoo Chat – although there are others.

Bullying via websites — use of defamatory blogs (web logs), personal websites and online personal "own web space" sites such as Bebo (which works by signing on in one's school, therefore making it easy to find a victim) and MySpace – although there are others.

'Flames' - unpleasant or unwanted emails