FULWELL JUNIOR SCHOOL

INFORMATION TECHNOLOCY POLICY

(Updated January 2014)

Including:

- **Mobile Phone Policy**
- **Cyber bullying Policy**
- **Computer Use Policy (Staff and Pupils)**
- **Internet Policy (Staff & Pupils)**
- **ICT Security Policy**

Introduction:

Fulwell Junior School acknowledges that Information Technology is an important element of modern education. It opens up opportunities for delivering the curriculum in innovative ways. However, the use of the many different mediums should be countered with safety controls to protect the integrity of pupils and staff alike.

Why have an Information Technology Policy?

- To protect the confidential data held on computer in school from loss and corruption;
- To ensure the ICT mediums at our disposal are used ONLY for the purposes of delivering educational resources and not for personal gain;
- To protect children against malicious and unpleasant media and teach them how to use information technology safely;
- To adhere to the Data Protection guidance regarding how information is stored and used.

Mobile Phone Policy:

See also the associated Risk Assessment (Pupil Safety and Wellbeing) for more detailed analysis of risk and control.

As a general guideline, mobile phones are **not** permitted in school.

In certain *exceptional* circumstances (parent illness or social care involvement for example), the school may be prepared to accommodate a child with a phone for a distinct reason and for a specified timescale, but only after full consultation with the Head Teacher or School Business Manager. On such occasions, phones will be retained in the school office at the beginning of the day, on the strict understanding that parents accept any loss/damage is at their own risk.

The school position on mobile phones in school will regularly be communicated to parents when lapses in the interpretation of this guidance occur; see the extract here from a letter issued 2009 and also the relevant section of the annual *School Prospectus 2013/14*.

'Mobile phones in the classroom are a distraction. It is an area of communication that we cannot effectively regulate. Phones with camera capabilities could also be used to the detriment of other children.
Teachers cannot take responsibility for looking after valuable property in the classroom, and many mobile phones are expensive. The school cannot be held responsible for any loss or damage that may be incurred as a result, and there is a risk that those children who do bring a phone to school are in a more vulnerable position than those who don't, as they are exposing themselves to opportunist loss/damage both inside and outside of school.
We appreciate that many young people have phones at their disposal these days, and as a means of personal communication, they do have their benefits. However, they are not allowed in school for the reasons stated here and we would therefore be very grateful if you could acknowledge our guidance.'

Cyber Bullying Policy: (To be read alongside Anti-Bullying Policy)

Fulwell Junior School take the safety of its pupils very seriously and recognizes that the ever changing world of information technology poses as many pitfalls as advantages.

This policy has been compiled in consideration of the latest Department for Education guidance regarding how to tackle and prevent bullying, using links to their recommended support sites of **Childnet International** www.childnet.com and **Beatbullying** www.beatbullying.org and the following excerpt is from the DFE website:-

DFE Guidance :- Cyber-bullying

"The rapid development of, and widespread access to, technology has provided a new medium for 'virtual' bullying, which can occur in or outside school. Cyber-bullying is a different form of bullying and can happen at all times of the day, with a potentially bigger audience, and more accessories as people forward on content at a click.

The wider search powers included in the Education Act 2011 give teachers stronger powers to tackle cyber-bullying by providing a specific power to search for and, if necessary, delete inappropriate images (or files) on electronic devices, including mobile phones. Separate advice on teachers' powers to search (including statutory guidance on dealing with electronic devices) is available.

*For more information on how to respond to cyber-bullying and how pupils can keep themselves safe, please refer to the **Childnet International** and **Beatbullying** websites"*

What is Cyberbullying?

Cyberbullying can be defined as the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else. It can be an extension of face to face bullying, with technology providing the bully with another route to harass their target. However, it differs in several significant ways from other kinds of bullying:

- the invasion of home and personal space
- the difficulty in controlling electronically circulated messages
- the size of the audience
- perceived anonymity
- and even the profile of the person doing the bullying and their target

As with the schools general definition of bullying, however, we believe it should involve the whole school community; in this way, awareness is raised and our stakeholders can 'buy-in' to our policies of tackling cyberbullying.

Cyberbullying is a sub-set or 'method' of bullying. It can be used to carry out all of the different 'types' of bullying (such as racist bullying, homophobic bullying, or bullying related to special educational needs or disabilities), but instead of the perpetrator carrying out the bullying in person, they use technology as a means of conducting the bullying. Cyberbullying can include a wide range of unacceptable behaviors, including harassment, threats and insults. And like face to face bullying, is designed to cause distress and harm.

Cyberbullying takes place between children; between adults; but also across different age groups. Young people can target staff members or other adults through cyberbullying.

Cyberbullying in the School Community:

Cyberbullying is not a new phenomenon, but as mobile phone and internet use become increasingly common, so does the use of technology to bully.

The School already address bullying, discrimination and behavioral issues as part of school policy. This guidance is designed to assist staff and parents in the interpretation of how the technology is being used, and the potential abuse that can be caused.

Only by open discussion with children parents and staff can the issue be shared and understood, what the consequences are and what the preventative measures can be.

Forms that cyberbullying can take:

Cyberbbullying takes different forms, some of which are harder to detect or less obviously associated with bullying than others; some are already included in the general bullying policy that the school operates, and there are already systems in place to deal with these:

1. *Threats and intimidation*: Serious threats can be sent to both staff and pupils by mobile phone, e-mail and via comments on social networking sites or message boards.
2. *Harassment or stalking*: Repeatedly sending unwanted texts or instant messages, or making phone calls; using public forums, such as message boards or chatrooms, to repeatedly harass or to post derogatory or defamatory statements in order to provoke a response from their target; tracking targets using spyware; sending viruses.
3. *Vilification/Defamation*: Cyberbullying can include posting upsetting or defamatory remarks about an individual online, or name calling using a mobile device.
4. *Ostracising/Peer Rejection/Exclusion*: Online exclusion can be harder to detect than children obviously being marginalized in a space, such as a classroom, where there are adults present. Social networking sites such as Facebook and Twitter provide a platform for young people to establish an online presence. They can be an important extension of a young persons social space and activity. It is possible for a group of students to set up a closed group, which can protect them from unwanted contact. It also means that excluding someone – by refusing to return or acknowledge messages, deleting them from their friendship lists or using 'ignore' functions - can be extremely hurtful.
5. *Identity theft, unauthorized access and impersonation:* Accessing and copying someone's information, for example e-mails or pictures, in order to harass or humiliate them; deleting someone's information; impersonating someone, for example pretending to be the person whose account has been hacked in order to post abusive comments and bad language.
6. *Publicly posting, sending or forwarding personal or private information or images:* Once electronic messages or pictures are made public, containing them becomes very difficult. Video or pictures can be passed between mobile phones, uploaded to web sites or posted to public video hosting sites. Websites are potentially viewable by millions of people; even after pages or comments have been removed, 'cached' copies may still be available. Creating, possessing, copying or distributing images of children and young people under the age of 18 which are of an indecent or sexual nature is illegal under the Protection of Children Act 1978. These images are illegal even if they were taken in 'fun' or by 'willing' parties. These laws also apply to indecent 'pseudo-photographs' – images which have not been taken but have been created or adapted, for instance using digital imaging software.
7. *Manipulation:* This is an often under-considered form of bullying, but unfortunately cases of it do exist. Examples include outing pressure on someone to reveal personal information or to arrange a physical meeting. This can be done by using online friendship status, for example, suggesting that a genuine friend would give out personal information.

Popular mediums for cyberbullying:
Mobile phones;
Instant messenger and voice over internet protocols
Chatrooms and message boards
E-mail
Web-cams
Social network sites
Video hosting sites
Virtual learning sites
Gaming sites, consoles and virtual worlds

How can Fulwell Junior School monitor and prevent cyberbullying:

We will take a proactive stance on co-ordinating responsibility for cyberbullying and work with parents and children to identify instances where it could occur, and take action where appropriate. Parents have a responsibility to be monitoring their child's activities with regard to access to social media and should consider the age of their child and the impact inappropriate access may have.

There is no single solution to the problem; it needs to be regarded as a live and ongoing issue. We consider that there are 5 essential action areas that together form an effective and comprehensive approach to prevention:

- Understanding and talking about cyberbullying and the wide issue of bullying, including the effects on others
- Updating existing policies and practices
- Making reporting cyberbullying easier
- Promoting the positive use of technology
- Evaluating the impact of prevention activities

Understanding & talking about cyberbullying:
It is an issue that is already on the school agenda, and is an important way of working towards the Every Child Matters outcomes, and safeguarding the health and wellbeing of the school community.

Promote awareness and understanding about cyberbullying:
We will work within the curriculum to highlight the different forms that cyberbullying can take, and make children aware of its impact. We will enforce this message by regular updates to parents, advising of what they should watch out for in their children's internet or mobile phone activities. This information will be displayed in the ICT suite in school to inform children of what they should do if they think they are the victim of cyberbullying, and who they can turn to for support.

Publishing sanctions:
It is also important that children and parents are alerted to the school policy on dealing with cyberbullying as it becomes evident, with the understanding that it will not be tolerated in school on any level. Pupils will be reminded of the

importance of a safe environment and how to behave responsibly when using ICT. The sanctions we choose to adopt for instances where cyberbullying is detected would be dependent on the level of the abuse.

Logging all cyberbullying incidents within the school environment:
We will keep appropriate records of any incidents of cyberbullying, alongside wider bullying, and monitor our prevention activities in connection with this. We will remind children of the importance of discussing any concerns they have with a member of staff, in confidence. Similarly staff and parents should be aware of the non-verbal signs of cyberbullying, such as anxiety, depression or fear, that would otherwise be unusual in a child. This may also involve subtle comments or changes in relationships with friends.

Promoting the positive use of technology:
ICT is increasingly recognized as an essential life skill, and embedding technology across the curriculum and in learning and teaching delivery provides opportunities and benefits for both learners and staff members.
We will work with children and staff to promote e-safety:

- Never give passwords to other people
- Change passwords regularly
- Do not upload images of children to websites under any circumstances
- Ensure pupil data held on computers is password protected
- Ensure firewalls and security centre updates are working effectively. When in doubt, advice can be sought from the EdIT Support Team.

Similarly we will ensure that:

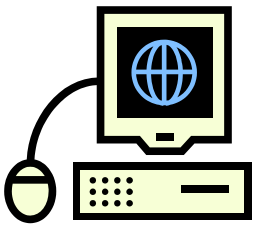
- Children only use the ICT resources in school for the purposes intended i.e. solely for educational use.
- All interactive resources are from reputable educational suppliers (Education City etc) and have been installed with full child-friendly firewalls/safeguards.
- Children cannot access chat rooms or social networking sites when using school computers; access to such sites is automatically prohibited by the server.
- Children are not given individual e-mail accounts; there is no facility in school for children to be sending each other messages by any medium.

Staff should reinforce the anti-cyberbullying code:

1. Always respect others
2. Think before you send
3. Treat your password like your toothbrush!
4. Block the bully!
5. Don’t retaliate or reply
6. Save the evidence
7. Make sure you tell

Summary

To protect the data held in files or Emails and to generally protect your computer from information loss or corruption



Why bother with protection?

All users have a duty to protect the School's assets.

School policy on privately owned IT equipment

It is Fulwell Junior Schools policy that ***privately owned*** IT equipment, which is to be used for work purposes or to be connected to the School's network or infrastructure, must be checked over, by a member of the ICT support team. Antivirus software must be up to date with the schools requirements. This does not include school assigned laptop PC's.

Security of computer equipment

The Schools network and the attached computers and peripherals have the highest priority.

If any problems are experienced, users should not attempt recovery – contact the Business Manager for assistance or use the ICT record book in suite to log complaints for the IT Support Technician.

It is the Schools data that is at risk!

Computer systems can be rebuilt, but only by authorised persons, not users.

Data is valuable: take care when saving and backing-up information.

Internet, intranet and Email

Always follow the policy, use the user guides for assistance.

Anti-virus software

Ensure your computer has the latest version installed. You may periodically be asked to bring your home-based lap top to school e.g. to ensure the most recent anti-virus software can be installed by the ICT technician.

Backups

To ensure that the important information is backed up regularly, copying to CD-ROM if necessary.

Do's and Don't's

Do:

- Use effective passwords
- Power down at cease of work
- Lock the PC when unattended
- Keep laptops secure when traveling or on a overnight stop.

Don't:

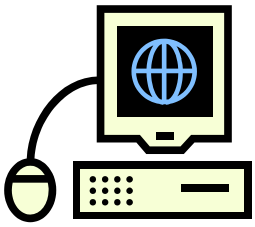
- Interfere with our PC's set-up
- Download software, wallpapers or screensavers from Internet.
- Illegally copy data or programs
- ***Use unauthorised software***
- Do not open any files attached to an email if the subject line is questionable or unexpected
- Do not access pornographic or obscene materials

Please familiarize yourself with the specific guidance regarding use of school Laptop computers : School owned ICT equipment is for school use ONLY and staff should not be downloading personal information (photo's/music etc) or browsing the internet with school merchandise.

You should ensure your login name and password are kept safe. You are responsible

Summary

Authorised use of the internet within the school is defined as using it for "Business purposes" only; this includes conducting valid research for work related matters.



Unauthorised use is defined as, but not necessarily limited to:

- Accessing offensive content of any kind, including pornographic material.
- Propagating a virus, worm, Trojan-horse, or trap door program.
- Disabling or overloading any computer system or network
- Circumventing any system intended to protect the privacy or security of another user.
- Promoting discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, or disability.
- Visiting Web sites that promote threatening or violent behaviour.
- Using the internet for illegal activities
- Distributing commercial messages.
- Accessing gambling or games web sites
- Downloading entertainment software or games, including MP3 or Video Streaming.
- Using online internet gaming.
- The use of chat websites and programs for example : msn messenger
- For personal finance gain
- Accessing/downloading non-business related videos and images.
- Forwarding E-mail chain letters.
- Downloading and distributing material protected under copyright laws without proper consent of the owner.
- Sending business-sensitive information using internet-based E-mail accounts unless authorised by the Head Teacher.
- Dispersing school data to pupils, parents or external agents without authorisation.
- Using the network to sign up to websites or organisations that offer rewards, monetary or otherwise, for surfing the internet.
- Downloading executable software, **unless** authorised by one of the ICT Support Staff.

User Accountability:

- Honouring acceptable use policies of networks accessed through the school's Internet services.
- Abiding by existing relevant legislation
- Following copyright laws protecting commercial software or intellectual property.
- Minimising unnecessary network traffic that may interfere with the ability of others, so as to make effective use of the schools network resources.
- Conducting yourself honestly and appropriately on the Internet, respecting copyrights, software licensing rules, property rights, privacy and prerogatives of others, just as you would in any other business dealing.
- Not overloading networks with excessive data or wasting the schools other technical resources.

Enforcement

Any employee found to have infringed this guidance may be subject to further action.

All authorized users should be made aware that the use of the Internet is monitored, and specific attention is drawn to the Laptop Declaration statements which all users are requested to sign. This prohibits the use of school owned ICT equipment for personal reasons, including internet access. Any breach of this guidance will be investigated and further action may be taken.

ICT INTERNET POLICY : PUPIL & STAFF SAFETY

The School has developed a set of guidelines for Internet use by both staff and pupils. These rules are made available to all staff and pupils, and kept under constant review.

All members of staff are responsible for explaining the rules and their implications. All members of staff need to be aware of possible misuses of on-line access and their responsibilities towards pupils.

By using the Schools Internet access facilities, both pupils and staff agree to abide by the following rules to ensure safe and secure access:

Internet Access

- Internet access is only provided and supported for educational purposes – i.e. research, class-work or homework. Whilst parental permission is not requested, the use of the facility is a privilege, not a right and access requires responsibility.
- ICT users should only access the system with their own personal username and password, and must not pass their password onto others
- Staff and pupils should understand that their Internet access is constantly monitored and logged, as a precautionary measure.
- It is a disciplinary offence to download or access material on the Internet of an offensive or inappropriate nature.
- Anyone abusing or suspected of abusing his or her right to access the Internet may have his or her Internet access withdrawn.

The Following are not permitted:

- Sending or displaying offensive messages or pictures
- Using obscene language
- Harassing, insulting or attacking others
- Damaging computers, computer systems or computer networks
- Violating copyright laws
- Using others passwords
- Accessing and/or deleting others folders work or files
- Intentionally wasting limited resources
- Downloading entertainment software or games or to play games against opponents on the internet
- Downloading images or videos unless there is a legitimate use for the school

Sanctions

- Violations of the above rules will result in a temporary or permanent ban on Internet use
- Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour
- When applicable, police or local authorities may be involved if particularly offensive material is found to have been downloaded.

Safety while "Online"

- Pupils should not pass on their personal details – name, address, telephone number, etc. – to other Internet users (e.g. via chat rooms, e-

mail, etc.) unless specifically asked to by a member of staff, for educational reasons.

- Pupils must immediately report any unpleasant materials or e-mail sent to them to a member of staff, or the Business Manager who will inform the appropriate Network Manager (EDiT Support in the first instance).

Be SMART

There's some great stuff on the Net, but some bad stuff too. It's important to be careful when using the Internet and remember these SMART rules! The rules can be applied when using PC's at school, but equally importantly when you use the Internet at home.

Keep your personal details **Secret**. Never use information without permission, and never give away your name, address, or passwords - it's like handing out the keys to your home!

Never **Meet** someone you have contacted in Cyberspace without your parent's/carer's permission, and then only when they can be present.

Don't **Accept** e-mails, open attachments or download files from people or organisations you don't really know or trust - they may contain viruses or nasty messages.

Remember that someone online may not be who they say they are. If you feel uncomfortable or worried in a chat room simply get out of there!

Tell your parent or carer if someone or something makes you feel uncomfortable or worried.

@ Copyright Internet Watch Foundation

Downloading of Files

- Pupils and staff should not use the Internet to download program files, either for installation on home PCs or on school machines. Installation or attempted installation of program files from sources not approved by the ICT Support department will be considered a disciplinary matter.
- Pupils and staff should not use the Internet for downloading music, audio or video files; unless it is relevant for coursework; this is due to the amount of excess network traffic which downloading this type of file generates.

ICT SECURITY POLICY:

There are many aspects of ICT security that have been touched upon in the information included within this general policy.

The issue of ensuring data stored on computers is safeguarded is important and at Fulwell Junior School, the following protocols have been introduced to ensure all information is stored in an appropriate environment, paying particular attention to Data Protection protocols and guidance issued by the Information Commissioners Office:

- Pupil data compiled by staff is held confidentially with security encryption and is password protected. Memory sticks must be password protected as standard as a portable storage medium, if there is any confidential information stored.
- Childrens work is saved on the curriculum server and cannot be accessed remotely other than by EdIT Support (for the purposes of checking any software problems etc.).
- Classrooms should be locked when staff are working on their computer and have to leave the room for any reason (PPA for example).
- All ICT equipment is security marked and logged in the permanent stock record.
- Firewalls and Security controls are in place for both the curriculum and administrative servers.
- Data on the server is 'backed-up' every evening by EdIT Support to ensure data can be retrieved in the event of accidental loss.
- Data stored on disc should be locked away in a secure cabinet and access restricted if the information is considered confidential.
- Data is protected as far as possible against virus infection/malicious content with the use of effective security detection (provided as standard through the EdIT support package), which is updated regularly.