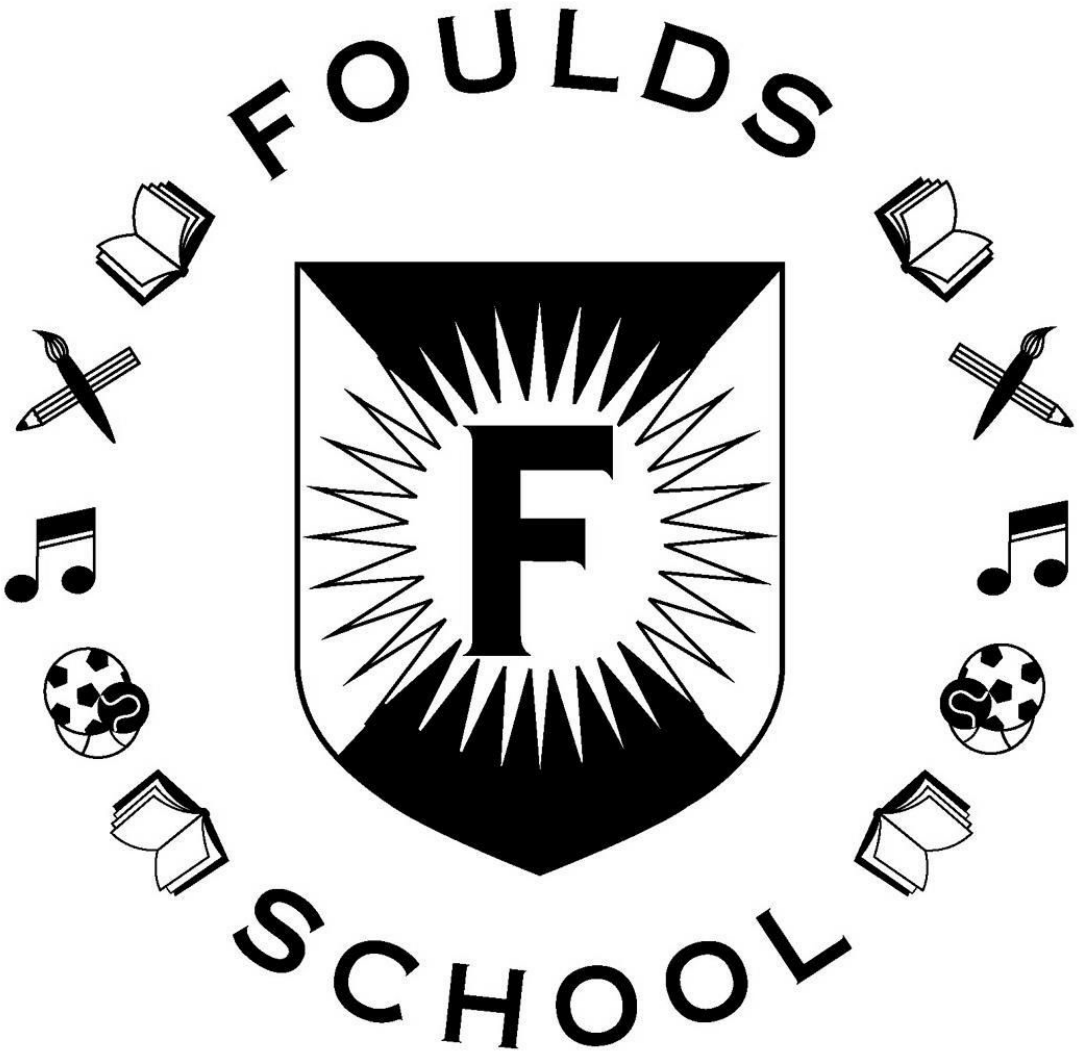
FOULDS PRIMARY SCHOOL



E-safety policy

Autumn 2018

This Policy replaces the E-safety policy of Autumn 2017 and will be reviewed in Autumn 2019. The Headteacher is responsible for the implementation and monitoring of this policy. The subject will be monitored by the Subject Leader in accordance with the School Development Plan. This policy should be read in conjunction with the Computing Policy and Safeguarding Policy (with regard to the taking and publishing of photographs of pupils).

E-safety Policy Contents

Further separate documents:
Acceptable Use - pupils – EYFS, KS1 and KS2
Acceptable Use – staff/governors
Acceptable Use – parents/carers
"What do we do if?" – guidance for staff
"Social Networking and Internet Hints and Tips" - guidance for adults

Section 1: Overview - The Acceptable Use of the Internet and related Technologies

a. **Context**
b. **The Technologies**
c. **Whole school approach to safe use in Computing**
d. **Roles and responsibilities**
e. **Communications**
f. **How will complaints regarding e-safety be handled**

a. Context

In England, schools are subject to an increased level of scrutiny by Ofsted Inspectors during school inspections - following the introduction of the new Framework and the Ofsted Briefing Document on E-Safety – http://www.ofsted.gov.uk/resources/briefings-and-information-for-use-during-inspections-of-maintained-schools-and-academies

NAACE SRF (Self Review Framework) elements – maintaining the ICT Mark

1b – Safeguarding
Foulds is aware of its responsibilities in ensuring that Computing usage by all network users is responsible, safe and secure.
There are relevant and comprehensive policies in place which are understood and adhered to by all network users.

2a **–** Effective and safe use of digital resources

Most pupils have a good range of skills that enable them to access and make effective use of digital resources to support their learning. They understand the issues relating to safe and responsible use of Computing and adopt appropriate practices

The Green Paper *Every Child Matters*[1] and the provisions of the *Children Act 2004*, *Working Together to Safeguard Children*[2] sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- safe from extremism and radicalisation
- secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use Computing in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that Computing can offer new weapons for bullies, who may torment their victims via websites or text messages and that sexting is a concern even in Primary; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour. Computing can also be used as a tool to expose children to extremism and potentially radicalise them.

It is the duty of Foulds to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to Foulds' physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

b. **The Technologies**

Computing in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include, for example:

- The Internet
- E-mail
- Instant messaging e.g. Snapchat, Kik, Whatsapp, BBM, often using simple web cams
- Blogs (an online interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites e.g. Facebook, Twitter, Instagram, LinkedIn
- Video broadcasting sites e.g. Youtube

[1] See The Children Act 2004 [http://www.opsi.gov.uk/acts/acts2004/20040031.htm]
[2] Full title: Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children.

- Chat Rooms e.g. Teenchat, HabboHotel, MovieStarPlanet, Tik Tok, Houseparty, Monkey
- Gaming Sites e.g. Club Penguin, Minecraft, Twitch, Discord, Fortnite
- Gaming consoles with online gaming e.g Xbox Live, Playstation Network
- Music download sites e.g. Itunes, Amazon
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications.
- Smart TVs

c. **Whole school approach to the safe use in Computing**

Creating a safe Computing learning environment includes three main elements at Foulds:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive E-Safety education programme for pupils, staff and parents.

d. **Roles and Responsibilities**

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of Foulds. The Headteacher, together with the Computing subject leader, ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to a member of the senior management team.

Our school **e-Safety Coordinator** is Rachel Gagnon

Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as NAACE and The Child Exploitation and Online Protection (CEOP)[3]. Foulds' e-Safety coordinator ensures the Head, senior management and Governors are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on e-Safety and are updated at least annually on policy developments to allow them to review the effectiveness of the policy.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms, ensuring pupils are given clear objectives for Internet use, taught what is acceptable and follow the school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with Foulds' Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- Publication of pupil information/photographs and use of website;
- GDPR regulations;

[3] http://www.ceop.gov.uk/

- E-Bullying / Cyberbullying procedures;
- Their role in providing e-Safety education for pupils.

Staff are reminded / updated about e-Safety matters at least once a year; this is a standing item on the Business agenda for September Inset. New staff are given the e-safety policy during induction.

E-safety is an integral part of the Computing Curriculum, under Digital Literacy. Pupils need to know how to control and minimise online risks and how to report a problem.

Foulds School makes every effort to engage with parents over e-safety matters and parents/guardians/carers are asked to sign and return an e-safety/AUP form when their child starts at Foulds and again at the start of KS2. In addition, the new school website (http://www.fouldsp.org) features an 'E-Safety' section in the 'Parents' Area.'

e) ***Communication***

How is the policy introduced to pupils?

- Instruction in responsible and safe use precedes Internet access.
- E-safety training is included in the Computing Scheme of Work covering both school and home use.

Many pupils are very familiar with the culture of new technologies. Pupils' perceptions of the risks may not be mature; the e-safety rules need to be explained or discussed.

E-safety is taught in all year groups, covering age-appropriate issues. Useful e-safety programmes include:

- Barnet and LGfL e-Safety and e-literacy Framework for EYFS-Y6 (https://www.lgfl.net/online-safety/default.aspx)
- Think U Know (www.thinkuknow.co.uk/)
- Grid Club (www.gridclub.com)
- SWGfL Digital Literacy and Citizenship (www.Digital-literacy.org.uk)
- CEOP (https://ceop.police.uk/)

How is the policy discussed with staff?

It is important that all staff feel confident to use new technologies in teaching. Staff will be given opportunities to discuss the issues and develop appropriate teaching strategies

Staff must understand the rules for information systems misuse. If a member of staff is concerned about any aspect of their Computing use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

Computing use is widespread and all staff including administration, caretaker, governors and helpers are included in appropriate awareness raising and training. Induction of new staff includes information about Foulds' e-Safety Policy. There are clear procedures for reporting issues.

How is parents' support enlisted?

Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. Foulds can help parents plan appropriate supervised use of the Internet at home.

- Internet issues are handled sensitively, and parents are advised accordingly.
- A partnership approach with parents is encouraged. This includes parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet are made available to parents eg through updates in the newsletter.

f) ***How are complaints regarding e-Safety handled?***

Foulds will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither Foulds nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview with class teacher, Deputy Headteacher or Headteacher;
- informing parents or carers;
- fixed term exclusion;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including work];
- referral to Barnet LA / Police.

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school and Barnet LA child protection procedures.

Section 2: Managing the Internet Safely

Foulds School:

- Does not allow pupils to use the internet unless they are supervised by an adult
- Maintains the filtered broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Works in partnership with the LA to ensure any concerns about the system are communicated to LGfL so that systems remain robust and protect students;
- Has additional user-level URL filtering in-place using the *Synetrix USO service.*

- Ensures network health through appropriate anti-virus software *Sophos / other* and network set-up so pupils cannot download executable files such as .exe / .com / .vbs etc.;
- Utilises caching as part of the network set-up;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies;
- Ensures the Systems Administrator / network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Uses individual log-ins to log-on and access Google Apps for Education
- Ensures that no member of staff ever sends personal data over the Internet other than through the school email or by uploading to Google Drive (through which data is secured by log-ins and 'sharing' folders/files with only those concerned) Communication of sensitive information to the LA is via USO-FX. Personal level data should not be taken off-site unless it is on an encrypted device.
- Uses 'safer' search engines with pupils and activates 'safe' search where appropriate;
- Ensures pupils only publish within appropriately secure learning environments such as their own closed secure LGfL portal or Learning Platform e.g. Google Drive work only shared with classmates/class teacher and webpages not published to the outside world.

Use of the Internet

Foulds School:

- Supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access.
- uses the pan-London LGfL Atomwide NetSweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- Staff should preview all sites before use [where not previously viewed and cached], including any 'comments sections' [e.g. when accessing youtube videos], to check for suitability. Alternatively, use sites accessed from managed 'safe' environments such as the LGfL content site or Espresso;
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs staff and students that that they must report any failure of the filtering systems directly to the Computing coordinator, who reports to LA / LGfL where necessary;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks social networking sites for specific purposes / Internet Literacy lessons;
- Only uses the LGfL / NEN (National Educational Network) service for video conferencing activity;
- Only uses approved or checked webcam sites;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes such as LGfL's Audio Network;

- Requires pupils (and their parent/carer) from EYFS, Key Stage 1 and 2, to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme;
- Uses closed / simulated environments for e-mail for pupils;
- Requires all staff and volunteers to sign an e-safety / acceptable use agreement form and keeps a copy on file;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures the named child protection officer has appropriate training;
- Ensures parents provide consent for pupils to use the Internet, as well as other Computing technologies, as part of the e-safety acceptable use agreement form at the time of their daughter's / son's entry to Foulds;
- Makes information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – the Police and Barnet LA.

Education and Training

Foulds School:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report abuse;
- Has a clear, progressive e-safety education programme throughout all Key Stages, built on Barnet LA and LGfL e-Safety curriculum framework (EYFS-Primary). Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:
    - to STOP and THINK before they CLICK
    - to discriminate between fact, fiction and opinion;
    - to develop a range of strategies to validate and verify information before accepting its accuracy;
    - to skim and scan information;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know some search engines / websites that are more likely to bring effective results;
    - to know how to narrow down or refine a search;
    - to understand how search engines work;
    - to understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;

- to understand how photographs can be inappropriate, manipulated and how web content can attract the wrong sort of attention;
- to understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files – such as music files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; online gaming / gambling;
- Ensures staff know how to encrypt data where the sensitivity requires and that they understand data protection and general Computing security issues linked to their role and responsibilities;
- Updates staff and/or makes training available to staff on the e-safety education program;
- Runs a programme of advice, guidance and training for parents, including:
  - Information leaflets; in school newsletters; on Foulds website;
  - demonstrations, practical sessions held at school;
  - distribution of 'think u know' for parents materials
  - suggestions for safe Internet use at home;
  - provision of information about national support sites for parents.

Section 3: Managing Email

Foulds School:

- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example office@fouldsp.org for any communication with the wider public.
- If one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law we may contact the police.
- Accounts are managed effectively, with up to date account details of users
- Staff members who have left the school are removed from the school email system.

- Messages relating to or in support of illegal activities may be reported to the authorities.
- Spam, phishing and virus attachment can make e-mail dangerous. We use filtering software to stop unsuitable mail. Suspected failure of software to filter potential spam, phishing emails or viruses to be reported to the Computing co-ordinator.

Pupils:

- We only use Google mail or Google Apps for Education mail with pupils.
- Pupils are introduced to and use e-mail as part of the Computing scheme of work.
- Pupils are taught about the safety and 'netiquette' of using e-mail i.e.
    - not to give out their e-mail address unless it is part of a school managed project or someone they know and trust and is approved by their teacher or parent/carer;
    - that an e-mail is a form of publishing where the message should be clear, short and concise;
    - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
    - they must not reveal private details of themselves or others in email, such as address, telephone number, etc;
    - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    - the sending of attachments should be limited;
    - embedding adverts is not allowed;
    - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
    - not to respond to malicious or threatening messages;
    - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
    - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
    - that forwarding 'chain' e-mail letters is not permitted;
- Pupils sign Foulds Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff only use Google Staffmail e-mail or the Google Apps for Education system for confidential information;
- Ensure that e-mail sent to an external organisation is written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow Foulds 'house-style';
    - the sending of attachments should be limited;
    - the sending of chain letters is not permitted;
    - embedding adverts is not allowed;
- Staff sign the appropriate school AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Additional support materials can be found at: www.esafety.lgfl.net

Section 4: Use of digital images

In Foulds school:

- The Headteacher, Deputy Headteacher and Computing co-ordinator take editorial responsibility to ensure that the website content is accurate, quality of presentation is maintained and complies with copyright;
- Uploading of information on the public website is restricted to Kim Sanett, Lynda Stoker and other members of staff as fits their role.
- Foulds website complies with Foulds' guidelines for publications;
- Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached (except Staff within the 'About Our School' section). Adults have the right to refuse permission to publish their image;
- Uploading of information on the school's network (Google drive) is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas
- We gain parental / carer permission for use of digital photographs or video involving their child as part of Foulds agreement form when their daughter / son joins Foulds. Parents have the right to refuse/limit permission for their child's work and/or image to be published/ Permissions are listed on the 'permission for photos or images latest update' spreadsheet, updated by the Office and distributed regularly to staff;
- Digital images / video of pupils are stored in staff Google drive folders or their school laptop and images should be deleted at the end of the year – unless an item is specifically kept for a key school publication, evidence for professional development or educational purposes within school;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to Foulds website;
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- We do not include names in the school newsletter when images accompany the article. Where names are used (when no images present), only the first name of the child is used. Children featured in newsletter images are checked against the 'permission for photos or images latest update' spreadsheet' before submission to ensure we have parental permission to publish as newsletters now are accessible to the world via the new website;
- Staff sign Foulds' Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- Pupils are only able to publish to their own 'safe' space on Google drive in school or on the Foulds Website;
- Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their Computing scheme of work;

- Pupils are taught about how images can be abused in their eSafety education programme;

Social networking (other than Foulds website):

- The schools will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.
- Any teachers' official blogs should be password protected and permission given by the Headteacher prior to publication. Teachers should be advised not to run social network spaces for student use on a personal basis.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.
- Schools should be aware that bullying can take place through social networking especially when a space has been set up without a password and others are invited to see the bully's comments.
- It is not appropriate for a member of staff to have links with a current pupil via a social networking site - please refer to Hints and Tips for further guidance, and use your professional judgement.

Section 5: Managing equipment

To ensure the network is used safely, Foulds school:

- Ensures staff read and sign that they have understood Foulds' e-safety Policy. Following this, they are set-up with email access and can be given an individual Google log-in username and password;
- Pupils log into Google Apps for Education with a class log-in or their own individual log in
- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find;
- Makes clear that no one should log-on as another individual user – if two people log on at the same time this may corrupt personal files and profiles;
- Has set-up the network with a shared work area for each class
- Requires all staff users to always log off when they have finished working or are leaving the computer unattended;
- Requests that staff and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO

switch the computers off at the end of the day and projectors when they are not being used e.g. between lessons, over lunch break.

- Has set-up the network so that users cannot download executable files / programs;
- Has blocked access to music download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus software maintained up-to-date and Foulds provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by Foulds is used solely to support their professional responsibilities. Laptops are marked with F codes unique to each item, an' Inventory' masterlist listing to whom each school laptop is issued and responsible for. This list is kept up-to-date by the Computing co-ordinator. Staff should inform the Computing co-ordinator if they wish to reallocate equipment;
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies e.g. Borough email or Intranet; finance system, Personnel system;
- Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by site manager / Technician; equipment installed and checked by approved Suppliers / LA electrical engineers;
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
- Does not allow any outside Agencies to access our network remotely except where there is a e.g. technical support or MIS support through LA systems;
- Provides pupils and staff with access to content and resources through the approved Learning Platform (Google Education apps and drive) which staff and pupils access using their USO
- Uses the LGfL USO-FX / DCSF secure s2s website for all CTF files sent to other schools, and the Perspective Lite system within the LA
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or sent within the approved secure system in our LA ;
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the school ICT systems regularly with regard to security.

Section 6: Electronic Devices – Searching and Deletion

The changing face of information technologies and ever increasing pupil / student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.
Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The Headteacher will need to authorise those staff who are allowed to carry out searches.
The Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices: the Headteacher, the Deputy Headteacher and, in their absence, the person left in charge of the school.

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Pupils are not allowed to bring mobile phones or other personal electronic devices into the classroom. Any such items must be left in the office in the morning and collected just before hometime.

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - Authorised staff may search with the pupil's consent for any item.
- Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996)

In carrying out the search:
The authorised member of staff must have reasonable grounds for suspecting that a pupil is in possession of a prohibited item.
The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search.
The authorised member of staff should take care that, where possible, searches should not take place in public places eg an occupied classroom, which might be considered as exploiting the student / pupil being searched.
The authorised member of staff carrying out the search must be the same gender as the pupil being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the pupil being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a pupil of the opposite gender including without a witness present, but **only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.**

Extent of the search:
The person conducting the search may not require the pupil to remove any clothing other than outer clothing. Outer clothing means clothing that is not worn next to the skin or immediately over a

garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).
'Possessions' means any goods over which the pupil has or appears to have control – this includes desks, lockers and bags.
A pupil's possessions can only be searched in the presence of the pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school code of conduct).

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- **child sexual abuse images (including images of one child held by another child)**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

Members of staff may require support in judging whether the material is inappropriate or illegal. One or more Senior Leaders should receive additional training to assist with these decisions. Care should be taken not to delete material that might be required in a potential criminal investigation.

The school should also consider their duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. There should be arrangements in place to support such staff. The school may wish to add further detail about these arrangements.

Section 7: How will infringements be handled

<u>Pupils</u>
Any pupil infringements will be dealt with initially by the class teacher and referred to the Computing subject leader or the Headteacher if the offence is repeated, is regarded as bullying or is of a serious nature e.g. deliberate mis-use of software/equipment.
Parents may be informed and sanctions imposed e.g. loss of a privilege.

<u>Staff</u>

In the case of an alleged infringement, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken. All sanctions are to be considered within the school's disciplinary procedures.

Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.
- Not implementing appropriate safeguarding procedures.
- Any behaviour on the World Wide Web that compromises the staff member's professional standing in the school and community.
- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software on network.

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, extremist, radical, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all Computing equipment by an outside agency, such as the school's managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in Foulds.
- Identify the precise details of the material.

Schools are likely to involve external support agencies as part of these investigations e.g. a technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Child Pornography

In the case of Child Pornography being found, the member of staff should be **immediately suspended** and the Police should be called: see the free phone number **0808 100 00 40** at: http://www.met.police.uk/childpornography/index.htm

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

http://www.iwf.org.uk

How will staff and pupils be informed of these procedures?

- They will be fully explained and included within Foulds' e-safety / Acceptable Use Policy. All staff will be required to sign Foulds' e-safety Policy acceptance form and to sign indicating that they have read this policy (including the 'Guidance: What do we do if?' and 'Using New Technology - Hints and Tips for adults working with children and young people' sections);
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate e-safety / acceptable use form;
- Foulds' e-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at Foulds.
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.

Inclusion
Foulds is committed to Equality of Opportunity in all aspects of school life. Equal opportunities in materials and teaching strategies will reflect the diversity in our world. See school's Equal Opportunities Policy.

Role of the SLT
- Developing, owning and promoting the e-safety vision to all members of Foulds community
- Supporting the development of an e-safety culture
- Making appropriate resources available to support the development of an e-safety culture
- Receiving and regularly reviewing e-safety incident logs
- Supporting the coordinator in the appropriate escalation of e-safety incidents
- Taking ultimate responsibility for e-safety incidents

Role of the coordinator
- Developing an e-safe culture and acting as a named point of contact for all e-safety issues
- Promoting e-safety to all groups of Foulds community
- Ensuring that e-safety is embedded within CPD for staff and across the curriculum
- Developing an understanding of the relevant legislation
- Liaising with the LA and other agencies as appropriate
- Reviewing and updating e-safety policies and practice on a regular basis.

Role of the teaching and support staff
- Contributing to the development of e-safety policies
- Reading and signing staff Acceptable Use Agreements and adhering to them
- Taking responsibility for the security of systems and data, which includes ensuring that all sensitive information is stored on an encrypted storage device
- Having an awareness of e-safety issues and how they relate to the children in their care
- Modeling good practice in using new and emerging technologies, emphasising positive learning opportunities rather than focusing on negatives
- Embedding e-safety education in curriculum delivery wherever possible
- Identifying individuals of concern and taking appropriate action
- Knowing when and how to escalate e-safety issues
- Maintaining a professional level of conduct in their personal use of technology, both within and outside school
- Taking personal responsibility for their professional development in this area

Role of parents and carers
- Contributing to the development of e-safety policies

- Reading Acceptable Use Agreements, encouraging their children to adhere to them, and adhering to them themselves where appropriate
- Using the school website and other network resources safely and appropriately
- Discussing e-safety issues with their children, supporting Foulds in its e-safety approaches and reinforcing their behaviours at home
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Modeling appropriate uses of new and emerging technologies
- Liaising with Foulds if they suspect, or have identified, that their child is conducting risky behaviour online

This policy was compiled by Helen Browett (2015) and updated by Rachel Gagnon (2018).

Guidance: What do we do if?

An inappropriate website is accessed <u>unintentionally</u> in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/e- safety officer and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered
4. Inform the LA if the filtering service is provided

An inappropriate website is accessed <u>intentionally</u> by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.
4. Inform the LA if the filtering service is provided

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the Head teacher and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the Head teacher should then:

- Remove the PC to a secure place.
- Instigate an audit of all ICT equipment by the schools ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in Foulds.
- Identify the precise details of the material.
- Take appropriate disciplinary action if appropriate
- Inform governors of the incident.

4. In an extreme case where the material is of an illegal nature:

- Contact the local police or High Tech Crime Unit and follow their advice.
- If requested to remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-safety anti-bullying and PSHE and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Inform the sender's e-mail service provider.
5. Notify parents of the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform the LA e-safety officer.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA e-safety officer.

An incident of sexting is reported.

1. Secure and preserve any evidence - no one to look at the evidence on their own/until advice has been taken.
2. Phone MASH and take advice
3. Inform the parent
4. Report to police if appropriate.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.
5. Inform LA e-safety officer.
6. Consider delivering a parent workshop for Foulds community.

All of the above incidents must be reported immediately to the Head teacher and e-safety officer.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

Using New Technology - Hints and Tips for adults working with children and young people

Read this, it might be helpful …

Social Networking hints and tips

Social networking sites are brilliant ways to stay in touch with friends and share photographs, comments or even play online applications such as chess or word games. However, they are also designed to enable advertisers to target you and entice you into buying goods and services based on the 'profile' information you reveal. Be web savvy!

- Social networking sites, such as Facebook, **have a range of privacy settings**. These are often set-up to 'expose' your details to anyone. When 'open' anyone could find you through a search of the networking site or even through a Google search. So, it is important to change your settings to "Just Friends" so that your details, photographs etc., can only be seen by your invited friends.
- Have a neutral picture of yourself as your profile image. Don't post embarrassing material.
- You do not need to accept friendship requests. Reject or ignore unless you know the person or want to accept them. Be prepared that you may be bombarded with friendship requests or 'suggestions' from people you do not know.
- Choose your social networking friends carefully and ask about their privacy controls.
- Do not accept 'friendship requests' on social networking or messaging sites from students, pupils or young people (or their parents) that you work with. Remember ex-pupils may still have friends at your school.
- Exercise caution – for example in Facebook if you write on a friends 'wall' all their friends can see your comment – even if they are not your friend.
- There is a separate privacy setting for Facebook groups & networks, you might have your profile set to private, but not for groups & networks. If you join a group or network everyone in the group or network will be able to see your profile.
- If you have younger family members on your social networking group who are friends with your students or pupils be aware that posts that you write will be visible to them.
- If you wish to set up a social networking site for a school project create a new user profile for this, do not use your own profile.
- If you or a friend are 'tagged' in an online photo album (Facebook, Flickr or similar) the whole photo album will be visible to their friends, your friends and anyone else tagged in the same album.
- You do not have to be friends with someone to be tagged in their photo album.
- If you are tagged in a photo you can remove the tag, but not the photo.
- Photo sharing web sites may not have privacy set as default.
- Your friends may take and post photos you are not happy about. You need to speak to them first, rather than contacting a web site. If you are over 18 the web site will only look into issues that contravene their terms and conditions.
- Once something is on the internet, even if you remove it, the chances are it has already been snapshotted by a 'web crawler' and it will always be there. Archives of web content are stored on sites like the WayBackMachine.
- Think about your internet use, adults are just as likely to get hooked on social networking, searching or games. Be aware of addictive behaviour!
- You will not be able to remove yourself completely from the Internet. 192.com has all the English electoral roles and for as little as £9.99 your personal information can easily be found by a stranger.

Wider Internet hints and tips

- Never tell anyone your password.
- Be careful how you choose passwords, most are very predictable. It is easy to find personal details online that might give password clues. It is recommended that you include capital letters, lower case letters and numbers – avoid birthdates, names, pets, addresses etc. It is best to avoid any work found in a dictionary.
- Keep all professional work and transactions completely separate from private. Create a web-based email account for private online business, such as online shopping and ensure you use your school / work email only for any professional communications.

- Create yourself a hotmail (or similar) account to use when searching for insurance quotes etc, when you are done either close the email account, or ignore it. Any junk mail generated will then not affect you.

- Be careful when form filling online…., do you know who the data is for? Only answer 'required 'questions, do not just give out information because you have been asked for it.

- Never verify banking details online.

- When you need to use a 'name' online consider what name you use. In a professional context you would probably use your full name, but in other contexts you may decide to use an alias to protect your identity. If so make sure it is appropriate.

- If you create a family tree and post it on the Internet, make sure your tree is set to private for anyone living or recently deceased (last 50 years). The information posted would be enough for someone to steal your identity and probably guess passwords and common security questions.

- If you get a phone call or an email from someone asking you to confirm personal details, (unless you are expecting the contact) do not give out any personal information.

- Popup adverts are often a nuisance. Close them carefully as a 'close' button will often lead you to more advertising as the 'X' might be a graphic.

- If you get an email or popup offer that seems too good to be true it probably is! Watch out for online cons – it is like online door step selling.

- If someone sets things up for you at home, make sure you change your password immediately. Someone with your username and password could impersonate you.

- If you think someone is impersonating you on Facebook or similar, report it. Impersonation usually breaches the terms and conditions – you will need to know the specific URL or user name, sites cannot work from a hunch.

- Cookies are not necessarily a bad thing. They save your surfing information and speed-up access to sites. However, if someone else has been surfing 'adult content' on your computer, the stored cookies may mean you get 'adult pop-ups and adverts'.

- Use legal sites for downloading music, films etc., such as iTunes.

- File sharing sites are not illegal but sharing of copyright material is. Downloading of illegal music and film downloading also leaves you at a huge risk of viruses. Even if you subscribe to a file sharing web site, such as Limewire, it does not mean that your downloading becomes legal.

- You can get Internet access from many games consoles and some MP3 players. Games with multiplayer features are often labelled as 'net play'. This means that you are playing with strangers online – the risks here are the same as for social networking, chatrooms and messengers.

- Applications like Skype and iplayer need bandwidth and can slow down the internet, particularly if you use a 3G mobile stick. Full screen iplayer could use up your allocation and your service may be 'throttled' - meaning you can only do some basic text work, searching and emails, but picture and video will not be possible.

- When you log-into a web site, unless your computer is exclusive to you, don't tick boxes that say 'remember me'.

- Don't leave yourself logged into your computer, software or websites. If you have to move away from your computer, log out.

- Don't give your username and password to anyone such as to a supply teacher / temporary member of staff – make sure your school has a guest login for visiting staff.

- Your school or work laptop (or other equipment) should not be used by friends and family.

If you work with young people:

- Try to provide pupils with direct links embedded into 'pages' in a document, London MLE 'room', or interactive whiteboard resource etc.

- If you do need to undertake Internet searches (including Internet image searches), rehearse before you use in class. Think about search terms. Even the most innocuous term can bring up adult material.

- Use child-friendly search engines with younger pupils. Older young people will use a variety of search engines at home; you are a role model for them in good use of a search engine. Look for opportunities to teach young people how to use search engines.

- When checking out web content make sure you are not displaying it on the interactive whiteboard or via a projector – research away from pupils.
- Watch YouTube (or any) videos before you use them in the classroom.
- If you use a YouTube (or any) videos, find out how to embed it using the 'Source' rather than a page link, as that exposes pupils to other content.
- If you cut and paste or save content from the Internet or other peoples files make sure you remove the hyperlinks embedded in the text, or attached to images.
- If you want to use a clip download it (if legal & copyright allows), it might not be there next time you look for it.
- If you use your own equipment in school (such as cameras or laptops), ensure senior leadership have given you permission and make sure that school files (photographs etc) are downloaded and stored in school, not at home.
- Do not take stored pupil photos or information home. If for any reason you need to ensure you have senior leadership's permission, and ensure it is on an encrypted device.
- Video Conferencing – you can be broadcasting without realising it, if you have VC in your classroom make sure it is switched off after use and that the camera is turned away from the class.
- You need to be a role model for copyright. Make sure you use multimedia resources appropriately, don't just 'grab stuff' off the Internet. Use the copyright images from the NEN, LGfL or other sites your school / LA has advised you of. You cannot show DVDs in school, although it is safe to use film trailers. But, make sure you download the right version, as there are can be more than one film trailer, including trailers for 'adult versions' of blockbusters.

Email hints and tips

- Keep all professional work and transactions completely separate from private. Create a web-based email account for private online business, such as online shopping and ensure you use your school / work email only for any professional communications.
- Create yourself a hotmail (or similar) account to use when searching for insurance quotes etc, when you are done either close the email account, or ignore it. Any junk mail generated will then not affect you.
- If you get an email from someone or a company that you have never head of and it asks you to reply to unsubscribe, don't. By unsubscribing you will verify that you exist. Just ignore the email. If they carry on emailing use email rules to block the sender.
- If you get emails that offer you money making schemes (e.g. the 'Nigerian email'), Russian wives, pharmaceutical products and body part enhancement don't be upset, you have not been personally targeted, this is spam and junk mail.
- Webmail is useful but insecure, and your email address is easily passed on.
- If you get spam or junk mail it does not mean that someone has 'hacked' into your email; people get email addresses in different ways, it might be a software 'guess' – a programme generates lots of possible emails and sends out millions of emails knowing that statistically some of them will be real. Software also searches web sites for email addresses and harvests them.
- Only open Email attachments from trusted sources, you won't get a virus from the initial email text, but it may be contained in an attachment.
- If emails from friends or acquaintances start to become unsuitable – say something before you receive something really problematic.
- Don't give out private email addresses to students and pupils.

Phone hints and tips

- Don't give out your mobile number or home number to students or pupils.
- If you have a Bluetooth phone do you know if Bluetooth is turned on or off? If it is on is there a password? Open un-passworded Bluetooth means anyone else with Bluetooth in range can read the content of your phone or device.
- Many hand held games consoles have wireless and Bluetooth and can be used to make contact from 'stranger' devices within range.