



## Child Online Safety Policy

Cooper & Jordan school believes that the use of information and communication technologies in schools brings great benefits. Recognising the child online safety issues and planning accordingly will help us to ensure appropriate, effective and safer use of electronic communications.

### **Why do we need a child online safety Policy?**

In today's society children interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place them in danger.

This child online safety policy covers issues relating to children as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children. The policy sets out our child online safety approach and identifies core principles which all members of the school community need to be aware of and understand.

### **About the policy**

The child online safety policy should be used alongside the school's policies for Safeguarding, Child Protection, Anti-Bullying, Promoting Positive Behaviour and Relationships and ICT.

The school has a child online safety Coordinator who will review the child online safety policy and its implementation annually. The School has a member of the Governing Body to take responsibility for Safeguarding, which incorporates child online safety.

### **Teaching and learning**

#### Why is Internet use important?

The rapid developments in electronic communications are having many effects on society. Cooper & Jordan school believes that;

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

### How does Internet use benefit education?

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment. Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries
- inclusion in the National Education Network which connects all UK schools
- educational and cultural exchanges between pupils worldwide
- vocational, social and leisure use in libraries, clubs and at home
- access to experts in many fields for pupils and staff
- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across networks of schools, support services and professional associations
- improved access to technical support including remote management of networks and automatic system updates
- exchange of curriculum and administration data with Walsall Local Authority and DfE
- access to learning wherever and whenever convenient

### How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The school will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff will guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

### How will pupils learn how to evaluate Internet content?

The quality of information received via radio, newspaper and telephone is variable and we recognise the need for children and staff to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills.

- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

## **Managing Information Systems**

### How will information systems security be maintained?

Cooper & Jordan school recognises that it is important to review the security of the whole system from user to Internet. This includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

ICT security is a complex issue.

Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

The security of our information systems is maintained by Walsall Local Education Authority, who take responsibility at borough level for security and internet filtering.

Cooper & Jordan will ensure that:

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

#### How will email be managed?

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits; interesting projects between schools in neighbouring villages and in different continents can be created, for example.

In the school context (as in the business world), email is not to be considered private and Cooper & Jordan reserves the right to monitor email, where necessary, to maintain the safety of pupils and staff. Staff should only use a school provided email account to communicate with parents/carers, pupils and other professionals for any official school business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

Email accounts of pupils and staff will not be provided in a format which can be used to identify both a pupil's full name and the school.

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

- Whole -class or group email addresses will be used for communication outside of the school where possible.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.
- Cooper & Jordan has a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by the Pupil Support Worker.
- Staff should not use personal email accounts during school hours or for professional purposes.

### How will published content be managed?

Publication of any information online will always be considered from a personal and school security viewpoint. Material such as staff lists or a school plan are published in the school handbook or on a secure part of the website which requires authentication.

- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

### Can pupils' images or work be published?

Still and moving images and sound add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount. Although common in newspapers, the publishing of pupils' names with their images is not acceptable. Published images could be reused, particularly if large images of individual pupils are shown.

The school will, where possible, employ strategies such as using relatively small images of groups of pupils or even using images that do not show faces at all. Personal photographs can be replaced with self portraits or images of pupils' work or of a team activity. Pupils in photographs will, of course, be appropriately clothed.

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Pupils work can only be published with their permission or the parents.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
- The School has a policy regarding the use of photographic images of children which outlines policies and procedures.

## How will social networking, social media and personal publishing be managed?

The Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes and some sites may be dubious in content. Pupils need to know about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All staff will be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

- The Local Authority controls our school's access to social media and social networking sites.
- 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 email addresses, full names of friends/family, specific interests and clubs etc.
- Staff will not use Social Media tools with students as part of the curriculum.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the headteacher.
- Pupils will be advised on security and privacy online and to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be warned to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Newsgroups will be blocked unless a specific use is approved.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

## How will filtering be managed?

Levels of Internet access and supervision will vary according to the pupil's age and experience. Access profiles at Cooper & Jordan are appropriate for all members of the school community. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily.

Access controls, which are managed by Walsall Local Authority, fall into several overlapping types (commonly described as filtering):

- Blocking strategies prevent access to a list of unsuitable sites.

- A walled garden or “allow list” restricts access to a list of approved sites. Such lists inevitably limit pupils’ access to a narrow range of content.
- Dynamic content filtering examines web page content or email for unsuitable words.
- Keyword lists filter search engine searches and URLs for inappropriate results and web addresses. Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject rated pages exceeding a threshold.
- URL monitoring records the Internet sites visited by individual users. Reports can be produced to investigate pupil access.
- Key loggers record all text sent by a workstation and analyse it for patterns.

Cooper & Jordan recognises that filtering is not 100% effective. There are ways to bypass filters (such as using proxy websites, using a device not connected to the network e.g. mobile phone).

Occasionally mistakes may happen and inappropriate content may be accessed. Children will always be supervised when using internet access at school. In addition, Internet Safety Rules are displayed, and pupils, staff and parents/carers will be educated about the risks online.

- The school’s broadband access will include filtering appropriate to the age and maturity of pupils. This is controlled by Walsall Local Education Authority.
- The school will work with Walsall Local Education Authority to ensure that the filtering policy is continually reviewed.
- If staff or pupils discover unsuitable sites, the URL will be reported to the school’s child online safety Coordinator who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Walsall Police or CEOP.

#### How will video-conferencing be managed?

Video-conferencing enables users to see and hear each other between different locations. This ‘real time’ interactive technology has many uses in education. Equipment ranges from small PC systems (web cameras) to large room-based systems that can be used for whole classes or lectures.

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses will not be made available to other sites.
- Videoconferencing contact information will not be put on the school Website.
- The equipment must be secure and if necessary locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.
- Responsibility for the use of the videoconferencing equipment outside school time will be established with care.

#### **Users**

- Pupils will ask permission from a teacher before making or answering a videoconference call.
- Videoconferencing will be supervised appropriately for the pupils’ age and ability.
- Parents and carers consent will be obtained prior to children taking part in videoconferences.
- Only key administrators will be given access to videoconferencing administration areas or remote control pages.

- Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.

## **Content**

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

## How are emerging technologies managed?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment will be undertaken on each new technology for effective and safe practice in classroom use to be developed.

Virtual online classrooms and communities widen the geographical boundaries of learning. Approaches such as mentoring, online learning and parental access are becoming embedded within school systems. Online communities can also be one way of encouraging a disaffected pupil to keep in touch.

The safety and effectiveness of virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites and other online tools such as Facebook, YouTube, Skype and Twitter. The registering of individuals to establish and maintain validated electronic identities is essential for safe communication, but is often not possible.

Video conferencing introduces new dimensions; webcams are increasingly inexpensive and, with faster Internet access, enable video to be exchanged across the Internet. The availability of live video can sometimes increase safety - you can see who you are talking to - but if inappropriately used, a video link could reveal security details.

New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access. This can offer immense opportunities for learning as well as dangers such as a pupil using a phone to video a teacher's reaction in a difficult situation.

Cooper & Jordan strives to keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies. For instance text messaging via mobile phones is a frequent activity for many pupils and families; this could be used to communicate a pupil's absence or send reminders for exam coursework. There are dangers for staff however if personal phones are used to contact pupils and therefore a school phone should be issued.

The inclusion of inappropriate language or images is difficult for staff to detect. Pupils may need reminding that such use is inappropriate and conflicts with school policy. Abusive messages will be dealt with under the school's behaviour and/or anti-bullying policies.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use Policy.

### How should personal data be protected?

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. At Cooper & Jordan, personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

### **Policy Decisions**

#### How will Internet access be authorised?

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff will read and sign the School Acceptable Use Policy before using any school ICT resources.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.

- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

At Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional supervised access to specific and approved online materials.

At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

#### How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Walsall Local Education Authority can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

#### How will the school respond to any incidents of concern?

child online safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Any potential concerns will be dealt with at a personal level.

Staff will help develop a safe culture by observing each other's behaviour online and discussing together any potential concerns. Incidents of concern may include unconsidered jokes and comments or inappropriate actions. Any illegal activity must be reported to the school Designated Child Protection Coordinator.

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, the school will determine the level of response necessary for the offence disclosed. The decision to involve Police will be made as soon as possible, after contacting the Walsall Safeguarding Children Team or if the offence is deemed to be out of the remit of the school to deal with.

- All members of the school community will be informed about the procedure for reporting child online safety concerns (such as breaches of cyberbullying, illegal content etc).
- The child online safety Coordinator will record all reported incidents and actions taken.
- The Designated Child Protection Coordinator will be informed of any child online safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage child online safety incidents in accordance with the school behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Walsall Safeguarding Children Team or escalate the concern to the Police.

- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Walsall Safeguarding Children team.

#### How will e-Safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- All e-Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the Walsall Safeguarding Children Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

#### How is the Internet used across the community?

Internet access is available in many situations in the local community. In addition to the home, access may be available at the local library, youth club, adult education centre, village hall, supermarket or cyber café.

- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for pupils who use the internet and technology whilst on the school site.
- The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

#### How will Cyberbullying be managed?

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's child online safety ethos.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time.

Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.

- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

#### How will Learning Platforms be managed?

An effective learning platform or learning environment can offer schools a wide range of benefits to teachers, pupils and parents, as well as support for management and administration. It can enable pupils and teachers to collaborate in and across schools, sharing resources and tools for a range of topics. It also enables the creation and management of digital content and pupils can develop online and secure e-portfolios to showcase examples of work.

- The child online safety co-ordinator and staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns about content on the LP may be recorded and dealt with in the following ways:
  - The user will be asked to remove any material deemed to be inappropriate or offensive.
  - The material will be removed by the site administrator if the user does not comply.
  - Access to the LP for the user may be suspended.
  - A pupil's parent/carer may be informed.
  - A visitor may be invited onto the LP by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.
  - Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

## How will mobile phones and personal devices be managed?

Mobile phones and other personal devices such as Games Consoles, Tablets, PDAs and MP3 Players etc. are considered to be an everyday item in today's society and even children in early years settings may own and use personal devices to get online regularly. Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features.

However, mobile phones can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged;
- Their use can render pupils or staff subject to cyberbullying;
- Internet access on phones and personal devices can allow pupils to bypass school security settings and filtering.
- They can undermine classroom discipline as they can be used on "silent" mode;
- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff.
- The use of mobile phones and other personal devices by pupils and staff in school is covered in the school Acceptable Use Policies.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from the Head Teacher.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in the Early Year department of school at all and within certain areas within the wider school site such as the changing rooms, toilets and swimming pools.

## Pupils Use of Personal Devices

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place until the end of the school day.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

## Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff should use a school phone where contact with pupils or parents/carers is required.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by the Headteacher in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Headteacher.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose unless permission has been given by the Headteacher.
- If a member of staff breaches the school policy then disciplinary action may be taken.

## **Communication of the Policy**

### How will the policy be introduced to pupils?

- All users will be informed that network and Internet use will be monitored.
- An e-Safety training programme will be delivered across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- e-Safety training will cover both safe school and home use.
- child online safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to child online safety education will be given where pupils are considered to be vulnerable.

### Useful e-Safety programmes include:

- 🔗 Think U Know: [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)
- 🔗 Childnet: [www.childnet.com](http://www.childnet.com)
- 🔗 Kidsmart: [www.kidsmart.org.uk](http://www.kidsmart.org.uk)
- 🔗 Orange Education: [www.orange.co.uk/education](http://www.orange.co.uk/education)
- 🔗 Safe: [www.safesocialnetworking.org](http://www.safesocialnetworking.org)

### How will the policy be discussed with staff?

The e-Safety Policy will only be effective if all staff subscribe to its values and methods. Staff will be given opportunities to discuss the issues and develop appropriate teaching strategies.

ICT use is widespread and all staff including administration, governors and volunteers will be included in awareness raising and training.

- The e-Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.

- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

#### How will parents' support be enlisted?

Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home.

- Parents' attention will be drawn to the school e-Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to child online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e-Safety at other attended events e.g. parent evenings and sports days.
- Parents will be required to sign an e-Safety/Internet agreement as part of the Home School Agreement.
- Parents will be required to read the school Acceptable Use Policy for pupils and discuss it's implications with their children.
- Parents will be made aware of their responsibility regarding posting other children from school on Social Networking sites.
- Information and guidance for parents on e-Safety will be made available to parents in a variety of formats.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.
- Interested parents will be signposted to relevant organisation for further information.

Staff Responsible: Keith Farquhar

Date of next review: July 2018

## child online safety Contacts and References

**CEOP** (Child Exploitation and Online Protection Centre): [www.ceop.police.uk](http://www.ceop.police.uk)

**Childline:** [www.childline.org.uk](http://www.childline.org.uk)

**Childnet:** [www.childnet.com](http://www.childnet.com)

**Click Clever Click Safe Campaign:** <http://clickcleverclicksafe.direct.gov.uk>

**Cybermentors:** [www.cybermentors.org.uk](http://www.cybermentors.org.uk)

**Digizen:** [www.digizen.org.uk](http://www.digizen.org.uk)

**EiS** - ICT Support for Schools and ICT Security Advice: [www.eiskent.co.uk](http://www.eiskent.co.uk)

**Internet Watch Foundation (IWF):** [www.iwf.org.uk](http://www.iwf.org.uk)

**Kidsmart:** [www.kidsmart.org.uk](http://www.kidsmart.org.uk)

**Teach Today:** <http://en.teachtoday.eu>

**Think U Know website:** [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

**Virtual Global Taskforce — Report Abuse:** [www.virtualglobaltaskforce.com](http://www.virtualglobaltaskforce.com)

**Walsall Safeguarding Children Board:** [www.wlscb.org.uk/wscbindex](http://www.wlscb.org.uk/wscbindex)