Coppice School
E-safeguarding Policy

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our children and young people with the skills to access life-long learning and employment, where applicable.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the Internet technologies some children and young people are using, both inside and outside of the classroom, include:

- Websites
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Coppice School we understand the responsibility to educate our pupils and staff on e-safeguarding issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies; in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile Internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, tablets, mobile phones, camera phones, PDAs and portable media players, etc).

Roles and Responsibilities

As e-safeguarding is an important aspect of strategic leadership within Coppice School, the Head teacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

This policy is to protect the interests and safety of the whole school community. It is linked to the following school policies: child protection/safeguarding, health and safety, curriculum and home school agreements,

E-Safeguarding Guidance to Coppice School Staff

All Coppice School staff should consider the following:

You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the education establishment or Council and your personal interests.

You must not engage in activities involving social media which might bring Coppice School into disrepute.

You must not represent your personal views as those of Coppice School any social medium.

You must not discuss personal information about pupils, their family members; Coppice School or Council staff and other professionals you interact with as part of your job on social media.

You must not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations, Coppice School or the Council. You should ensure that at all times that you are not offensive, obscene, and discriminatory or harass others.

You must be accurate, fair and transparent when creating or altering online sources of information on behalf of Coppice School or the Council.

You should ensure that you do not misuse confidential, sensitive or copyrighted information.

PERSONAL USE OF SOCIAL MEDIA

Staff should be aware that social network sites are not private and anything published on them is considered in the public domain. Your personal use of social media is not considered to be totally outside of the work domain and depending on your actions you may face disciplinary action at work for your personal use of social media.

Staff members must not identify themselves as employees of Coppice School Council or service providers Coppice School in their personal web space. This is to prevent information on these sites from being linked with the education establishment and the Council and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services.

Staff members must not have contact through any personal social medium with any pupil, whether from Coppice School or any other education establishment, unless the pupils are family members. Staff members must decline 'friend requests' from pupils they receive in their personal social media accounts.

Coppice School does not expect staff members to discontinue contact with their family members via personal social media once the education establishment starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way.

Staff members must not have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.

On leaving Coppice School's service; staff members must not contact Coppice School pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former education establishments by means of personal social media.

Information staff members have access to as part of their employment, including personal information about pupils and their family members, colleagues Council staff and other parties and education establishment or Council corporate information must not be discussed on their personal web space.

Photographs, videos or any other types of image of pupils and their families or images depicting staff members wearing education establishment or Council uniforms or clothing with education establishment or Council logos or images identifying sensitive education establishment or Council premises (e.g. care homes, secure units) must not be published on personal web space.

Education establishment or Council email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

Staff members must not edit open access online material including but not limited to online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

Coppice School or Council corporate, service or team logos or brands must not be used or published on personal web space

Coppice School only permits limited personal use of social media while at work. Access to social media sites for personal reasons is not allowed between 9am and 5pm. There is a daily quota of 30 minutes to access these sites outside these hours. However, staff members are expected to devote their contracted hours of work to their professional duties and, in practice, personal use of the internet should not be on the education establishment's time unless using a mobile device during recognised breaks.

Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place.

Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

Guidance on Using Social networks responsibly – e.g. Facebook, Twitter, Instagram

Coppice School is committed to promoting the safe and responsible use of the Internet and student's access to social media sites can be a concern. Whilst pupils cannot access social networking sites at Coppice, they could have access to it on any other computer or mobile technology. Websites such as Facebook, twitter, instagram etc offer good communication and social connections, however they are created with their audience in mind and this is specifically 13 years old. Possible risks for children under 13 using the site may include:

Facebook use ‘age targeted’ advertising and therefore your child could be exposed to adverts of a sexual or other inappropriate nature, depending on the age they stated they were when they registered.

Children may accept ‘friend requests’ from people they don’t know in real life which could increase the risk of inappropriate contact or behaviour (grooming).

Language, games, groups and content posted or shared on Facebook is not moderated, and therefore can be offensive, illegal or unsuitable for children.

Photographs shared by users are not moderated and therefore children could be exposed to inappropriate images or even post their own.

Underage users might be less likely to keep their identities private and lying about their age can expose them to further risks regarding privacy settings and other options.

Facebook could be exploited by bullies and for other inappropriate contact.

Facebook cannot and does not verify its members therefore it is important to remember that if your child can lie about who they are online, so can anyone else.

Coppice School feels that it is important to point out to parents/carers the risks of underage use of such sites, so you can make an informed decision as to whether to allow your child to have a profile or not. These profiles will have been created away from the education establishment and sometimes by a child, their friends, siblings or even parents. Coppice will take action (such as reporting aged profiles) if a problem comes to our attention that involves the safety or wellbeing of any of our children. Should you decide to allow your children to have a social networking profile we strongly advise you to do the following:

Check their profile is set to private and that only ‘friends’ can see information That is posted;

Make sure they have privacy settings on to a high standard so they have to accept ‘tags’ in posts and pictures.

Remove the location/GPS setting on accounts, this can pin point to their friends

exactly what road they’re stood on when writing something on a social network.

Monitor your child’s use and talk to them about safe and appropriate online behaviour such as not sharing personal information and not posting offensive messages or photos;

Ask them to install the CEOP (Child Exploitation and Online Protection Centre) application from www.facebook.com/clickceop on their profile. This places a bookmark on their profile to CEOP and the ‘Report Abuse’ button which has been known to deter offenders;

Have a look at the advice for parents/carers from Facebook www.facebook.com/help/?safety=parents

Set up your own profile so you understand how the site works and ask them to add you as a friend on their profile so you can keep track of what they are posting online;

Make sure your child understands the following rules:

- Always keep your profile private;
- Never accept friends you don’t know in real life;
- Never post anything which could reveal your identity;
- Never post anything you wouldn’t want your parents to see;

- Never agree to meet someone you only know online without telling a trusted adult
- Always tell someone if you feel threatened or someone upsets you.

We recommend that all parents/carers visit the CEOP ThinkuKnow website for more information on keeping your child safe online or to report online abuse please see link below:

http://ceop.police.uk/safety-centre/

Managing Coppice School's e-safeguarding messages

We endeavour to embed e-safeguarding messages across the curriculum whenever the Internet and/or related technologies are used.

E-safeguarding in the Curriculum

Coppice School provides opportunities within a range of curriculum areas to teach about e-safeguarding as appropriate.
Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise.
Some pupils may be aware of the impact of online bullying and know how to seek help if they are affected by these issues.
Coppice School will send out relevant e-safeguarding information for parents/carers through newsletters, website and letters as appropriate.

Cyber-bullying

All elements referring to cyber-bullying are dealt with in the Coppice School's Anti-Bullying policy

E-safeguarding information for parents/carers

Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g., on school website.)

As and when the school are informed of a current topic / trend whereby children are /may be at risk school would inform parents.

Password Security

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood Coppice School's e-safeguarding Policy.
Staff users can be provided with an individual network and email.
If it is suspected that a password may have been compromised this should be reported to the Head teacher.
Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, including ensuring that passwords are not shared and are changed periodically.

Data Security

The accessing of school data is something that Coppice School takes very seriously. Staff are aware of their responsibility when accessing school data. They must not:

- access data outside of school
- take copies of the data
- allow others to view the data
- edit the data unless specifically requested to do so by the Head teacher and/or Governing Body.

Managing the Internet

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

Coppice School ensures pupils will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.

Staff will preview any recommended sites before use.

Raw image searches are discouraged when working with pupils.

All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

All users must observe copyright of materials from electronic resources.

Infrastructure

Doncaster Local Authority has a monitoring solution where web-based activity is monitored and recorded.

School internet access is controlled through the LA's web filtering service.

Coppice School is aware of its responsibility when monitoring staff communication under current legislation and takes into account:

- Data Protection Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998.

Staff are aware that school based email and Internet activity can be monitored and explored further if required.

If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to Mark Jarred, ICT Coordinator.

Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software.

It is not Coppice School's responsibility nor the ICT support company, to install or maintain virus protection on personal systems.
Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Head teacher who will decide if the technician should install it.
If there are any issues related to viruses or anti-virus software, the ICT support technician should be informed through the ICT maintenance form.

Publishing pupil's images and work

Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site, prospectus, displays around school etc. This consent form is considered valid for the entire period that the child attends Coppice unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.
Parents/carers may withdraw permission, in writing, at any time.
Pupils' names will not be used on the school website; particularly in association with photographs.
Parents will be asked for consent when photographs are to be used or taken by the press because their circulation and coverage may be local, national and sometimes international.
Pupil's work can only be published with the permission of the pupil, if appropriate, and parents and will not enable them to be individually identified.
Coppice will ensure that any photograph should not allow an unauthorised person to identify a child or their whereabouts, so, if a full name is used there will be no photograph, if a photograph is used there will be no full name.
Where children are in vulnerable circumstances (i.e. in care or victims of parental violence) they will not be photographed at all unless there is clear consent and no risk.

Photographs taken by parents/carers for personal use

In the event of parents/carers wanting to take photographs for their own personal use, Coppice School will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites. (E.g. school plays)

Social networking and personal publishing

Coppice School will block/filter access to social networking sites.
Newsgroups will be blocked unless a specific use is approved.
Pupils (where appropriate) and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However we accept that some pupils will still use them; they will be advised never to give out personal details of any kind which may identify them or their location.

Pupils (where appropriate) are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
Coppice pupils (where appropriate) are asked to report any incidents of bullying to the school.
School staff are advised not to add children as 'friends' if they use these sites. (Staff Code of Conduct)

Mobile technologies

Many new and existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to some children outside school. Some devices now offer open access to the internet and therefore open up risks associated with unregulated internet access.
Emerging technologies will be examined for educational benefit and the risks assessed before use in school is allowed.
Coppice School allows staff to bring in personal mobile phones and devices for their own use.
Under no circumstances does Coppice School allow a member of staff to contact a pupil or parent/carer using their personal device.
Pupils are not allowed to bring personal mobile devices/phones to school.
Any phones/devices that are brought in will be looked after by the class teacher until the end of day.

Assessing risks

Coppice School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor DMBC can accept liability for the material accessed, or any consequences of Internet access.
Coppice School will periodically audit ICT provision to establish if the e-safeguarding policy is adequate and that its implementation is effective.

Handling e-safeguarding complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.
Any complaint about staff misuse must be referred to the Head teacher.
Depending on the seriousness of the offence; investigation by the Head teacher/LA may involve immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
Complaints of a child protection nature must be dealt with in accordance with Coppice School's safeguarding procedures.
Parents will be informed of the complaints procedure.