COOKRIDGE HOLY TRINITY PRIMARY SCHOOL

E Safety and Social Media GUIDANCE FOR SCHOOL BASED STAFF

Adopted by Cookridge Holy Trinity Governing Body 2014

Updated and Amended by Governors and Computing Leader December 2017

Next review date: January 2019

To be used in conjunction with Internet Policy and Acceptable Use Policies.

Marita Sorial & Nicola Coward
HR Schools Team – 2014

CONTENTS

Marita Sorial & Nicola Coward
HR Schools Team – 2014

Introduction

"Children learn through exploration and natural curiosity, and it is part of our job as parents and carers to encourage that. However, as our children grow up, develop and discover new experiences, we have to take more and different steps to ensure their safety. Until their understanding and instincts catch up with their curiosity, our children need to be protected from everyday dangers – whether crossing the road, in and around the home, trying new foods or talking to new people they meet.

And sooner or later … going online."

www.getsafeonline.org, 2015

Section 1

Overview

ICT and the internet are essential tools for learning and communication that are used in Cookridge Holy Trinity Primary School to deliver the curriculum, and to support and challenge the varied learning needs of its students . ICT is used to share information and ideas with all sections of the school community.

At Cookridge Holy Trinity the use of the internet and ICT is seen as a responsibility and it is important that students and staff use it appropriately and practice good e safety. It is also important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.
E safety covers the use of the internet as well as mobile phones, electronic communications technologies and the use of social media and social networks. We know that some adults will use these technologies to harm students. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. All staff members have a 'duty of care' to ensure that students are educated about e-safety, know how to reduce risk of harm and stay safe, are able to report abuse and know who to talk to about any concerns around the use of this technology. There is also a duty to ensure that staff conduct does not bring into question their suitability to work with students.

This guidance takes into account the principles of the Safer Working Practice Guidance (HR Schools 2014), 'Keeping Children Safe in Education' (DfE, 2016) as well as guidance from the Department for Education (Safeguarding Children

in a Digital Work) and CEOP (Child Exploitation and Online Protection). This guidance also works alongside the 'LSCB Multi-Agency E-Safety Guidance' July 2016 and the schools 'Acceptable Use' policy November 2017.

Staff members have a responsibility in accordance with 'Keeping Children Safe in Education' (DfE, 2016) to safeguard students and report abuse immediately to designated staff members, as per the school's Child Protection Policy. Every member of staff will attend child protection training which outlines forms of abuse, and includes the indicators and signs of CSE.

This guidance applies to all staff employed either directly or indirectly by Cookridge Holy Trinity as well as volunteers and staff not employed directly by the school but based at the school. This guidance is also in conjunction with the school's Internet Policy (2017) and Acceptable use policy (2017). All staff are expected to adhere to this code of practice to ensure the safety of the students, young people and adults at risk who they may come into contact with through their professional role. Any member of staff found to be in breach of these guidelines may be subject to disciplinary action.

Definition of Students :

Throughout this document references are made to students. For the purpose of this documents this term refers to all children, young people and adults at risk, whom a professional may come into contact with, as a direct result of their professional role.

Adult At Risk: means adults who need community care services because of mental or other disability, age or illness and who are, or may be unable, to take care of themselves against harm or exploitation. The term replaces "vulnerable adults".

Section 2

Responsibilities

Staff are responsible for their own actions and must act, and be seen to act, in the best interests of children at all times. Staff must ensure they understand and adhere to this guidance as well as Cookridge Holy Trinity's code of conduct and Internet Acceptable Use Policy. Staff are responsible for acting promptly to

prevent and safeguard children from potential abuse online and for reporting any concerns in accordance with the Child Protection Policy and Procedures.

Staff are solely responsible for any content on their own personal social media networks and electronic devices. This means that staff are responsible for managing their own applications and content to ensure that it does not breach the school's safer working practice guidance, or undermine public confidence in the school or the education profession. Staff are personally responsible for security and privacy settings when using social media via their chosen equipment and as such failing to ensure adequate and appropriate settings are in place may lead to disciplinary action should the content be found to breach school expectations of professional conduct by bring the school into disrespect

Staff are also responsible for ensuring their own use of ICT and social media is professional and appropriate at all times. Staff must be aware that their conduct online, both inside and outside of school, must not breach the school's code of conduct or professional expectations. Any behaviour that is deemed to breach such expectations may be subject to disciplinary action.

Section 3

Social Contact withStudents.

Staff must not establish or seek to establish social contact with students, for the purpose of securing a friendship or to pursue or strengthen a relationship. Even if a student themselves, seeks to establish social contact. If this occurs coincidentally, the member of staff should exercise their professional judgement in making a response and be aware that such social contact could be misconstrued. Staff should alert the Headteacher of any such contact immediately.

All contact with students should be through appropriate channels at all times and should be within clear and explicit professional boundaries. This means staff should only contact students in school, using school equipment and regarding school matters, with appropriate permission from senior leadership.

Staff should not give, nor be required to give, their personal details such as home or mobile number, social media identities or personal email addresses to students. Any member of staff found to be in contact with students through any of the above means, or any other unapproved method, without prior consent of the head teacher/senior leader may be subject to disciplinary action.

Internal email and approved contact systems should only be used in accordance with the appropriate ICT policy and/or acceptable use policy.

Section 4

Social Media

Staff should not have contact with students using social media, and specifically social networking sites without prior permission of the Headteacher. Staff must not add students as friends or respond to friend requests from students. If a member of staff suspects that an existing friend is a student, child or young person, they must take reasonable steps to check the identity of the individual and end the friendship.

It is recognised that personal access to social networking sites outside the work environment is at the discretion of the individual however members of staff should consider their use of social networks as they take on the responsibilities of a professional, taking particular care to secure personal information and ensure their use of such networking sites is respectable and appropriate at all times.

Staff must ensure that their use of ICT and social media is professional at all times, even if this is outside of the school day, and that behaviour which breaches the School's code of conduct could lead to disciplinary action. Secure and suitable strength passwords should be devised and security settings should be applied to access your profile and the information contained is limited to those explicitly given access. It is also advisable to log out of any sites on a personal computer or an application on a mobile device to ensure maximum security.

Understand and check your privacy settings on your social media profiles so you can choose to limit who has access to your data. You may also want to consider how much personal information you include on your profile.

Personal profiles on social networking sites and other internet posting forums should not identify your employer or place of work and careful consideration should be given to information which is published on such sites. For example, information which is confidential, damaging to the school or undermines public confidence in the school's reputation.

All postings to social media websites should be considered in the public domain. Therefore, only post comments, videos and pictures which you would be happy to share with any group of friends, strangers or colleagues.

Material published by staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of a student, colleagues or member of the school community will be dealt with under the disciplinary procedure.

Inappropriate Material

When considering what is defined as inappropriate material it is important to differentiate between inappropriate and illegal and inappropriate but legal. All staff should be aware that in the former, case investigation may lead to criminal investigation, prosecution dismissal and barring. In the latter it can still lead to disciplinary action, dismissal and barring even if there is no criminal prosecution.

Illegal Material

It is illegal to possess or distribute indecent images of a person under 18 and viewing such images on-line may constitute possession even if not saved. Accessing indecent images of children on the internet, and making, storing or disseminating such material is illegal and if proven could lead to consideration of the individual being barred from work with students.

Material which incites hate, harm or harassment

There are a range of offences in relation to incitement of hatred on the basis of race, religion, sexual orientation and particular offences concerning harassing or threatening individuals which includes cyber bullying by mobile phone and social networking sites etc. It is an offence to send indecent, offensive or threatening messages with the purpose of causing the recipient distress or anxiety.

Professionally Inappropriate Material

A person should not use equipment belonging to their organisation to access adult pornography, as this is considered inappropriate material; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with students.
Individuals need also to be mindful of actions outside the work place that could be considered so serious as to fundamentally breach the trust and confidence in the employee, which could also result in disciplinary action.. Some examples of inappropriate material and actions are:

- Posting offensive or insulting comments about colleagues on social networking sites;
- Accessing adult pornography on work based computers during break;
- Making derogatory comments about students or colleagues on social networking sites;
- Posting unprofessional comments about one's profession or workplace on

social networking sites;
- Making inappropriate statements or asking inappropriate questions about students on social networking sites;
- Trading in fetish equipment or adult pornography;
- Contacting students by email or social networking without senior staff approval.

Section 6

Creating Images of Students through Video or Photography

Many work based activities involve recording images and these may be undertaken as part of the curriculum, extra school activities, for publicity, or to celebrate achievement. However, written permission must be gained from legal guardians as well as senior management prior to creating any images of students..

Using images of students for publicity purposes requires the age-appropriate consent of the individual concerned and their legal guardians. Images should not be displayed on websites, in publications or in a public place without such consent. The definition of a public place includes areas where visitors to the school or service provision have access.

Photograph or video images must be created using equipment provided by the work place. It is not acceptable to record images of students on personal equipment such as personal cameras, mobile phones or video camera. Images of students must not be created or stored for personal use.

Members of staff creating or storing images of students using personal equipment without prior consent will be subject to disciplinary action.

Members of staff must:

- be clear about the purpose of the activity and about what will happen to the photographs when the lesson/activity is concluded;
- ensure that senior management is aware that photography/image equipment is being used and for what purpose;
- ensure that all images are available for scrutiny in order to screen for acceptability;
- be able to justify images of students in their possession;
- avoid making images in one to one situations.

Members of staff must not take, display or distribute images of students unless they have consent to do so. Failure to follow any part of this code of practice may result in disciplinary action being taken.

For further guidance on creating, displaying and storing images of students please refer to the Safer Working Practice Guidance (HR Schools 2014) as well as guidance

from the Department for Education (Safeguarding Children in a Digital Work) and CEOP (Child Exploitation and Online Protection).

Section 7

Use of personal technology/equipment in school

The use of any personal equipment in schools should always be with the prior permission of senior management in order to comply with health and safety regulations, safer working practice guidance, data protection and school policies. Members of staff should take care to comply with acceptable use and ICT policies.

Personal equipment capable of recording images, moving images or sounds and those used for accessing the internet such as mobile phones, cameras, video cameras and laptops should not be used in work time without the prior permission of senior management.

Any member of staff found to be using such personal equipment without prior authorisation may be subject to disciplinary action.

Section 8

Internet Use

Members of staff must follow and adhere to the policies on the use of IT equipment at all times and must not share logins or password information with other members of staff, students, children or young people, friends, family or members of the public.

Under no circumstances should members of staff in the work place access inappropriate images using either personal or work based equipment. Accessing indecent images of children on the internet and making, storing or disseminating such material is illegal and if proven will invariably lead to disciplinary action the individual being barred from work with children and young people.

Using work based equipment to access inappropriate or indecent material, including adult pornography, either in the work place or at home, will give cause for concern particularly if as a result students or young people might be exposed to inappropriate or indecent material and may also lead to disciplinary action.

Section 9

Confidentiality and Security

Members of staff may have access to confidential information about students and the organisation in order to undertake their everyday responsibilities and in some circumstances this may be highly sensitive or private information. Such information

should never be shared with anyone outside the school, a member of the public or outside agencies, except in specific circumstances, for example when abuse is alleged or suspected. I
Only authorised school based devices and systems should be used to store and transfer confidential information Standard unencrypted email should **never** be used to transmit any data of a personal or sensitive nature. Staff that wish to use email to transfer such
data must ensure that personal or sensitive information is encrypted either through file encryption or through the use of a secure email facility which will encrypt the data (including any attachments) being sent. Members of staff found to be compromising confidentiality by use of unauthorised systems and devices could be subject to disciplinary action.

The storing and processing of personal information about students is governed by the Data Protection Act 1998. For further guidance in relation to confidentiality issues and safe storage of data please refer to the Safer Working Practice guidance document (2014).
Do we need to refer to the safe transfer of sensitive information set up and authorised by the LA or other organisations?

Section 10

Cyber Bullying

All forms of bullying, including cyber bullying, are taken very seriously. Bullying is never tolerated and it is not acceptable for any member of staff to behave in a manner which is intimidating, threatening or in any way discriminatory. Behaviour which constitutes Bullying or Harassment may be dealt with under the Grievance/Bullying and Harassment Policy and could result in disciplinary action.

However, this doesn't just extend to behaviour within the work place. In some instances bullying or harassment that occurs outside the workplace where there is a link to employment could also fall under the responsibility of the employer and therefore result in disciplinary action being taken against the responsible individual.

Certain activities relating to cyber bullying could be considered criminal offences under a range of different laws. Cyber bullying consists of threats, harassment, embarrassment, humiliation, defamation or impersonation and could take the form of general insults, prejudice based bullying or discrimination through a variety of media. Media used could include email, Virtual Learning Environments, chat rooms, web sites, social networking sites, mobile and fixed-point phones, digital cameras, games and virtual world sites.

If an allegation is received that a member of staff is responsible for comments made online which could be deemed harmful, threatening, defamatory, abusive or harassing in any way towards another employee, the school will investigate this

matter. Any allegation of bullying or harassment made by an employee against another member of staff where the accused uses the internet, mobile phone, text message or email, along with any other forms of abuse, may be dealt with through the Grievance/Bullying and Harassment Policy and could lead to disciplinary action.

Staff are required to take steps to protect themselves and their personal information by:

- Keeping all passwords secret and protect access to their online accounts
- Not befriending students and young people on social networking services and sites
- Keeping personal phone numbers private
- Not using personal phones to contact parents and students and young people
- Keeping personal phones secure, i.e. through use of a pin code.
- Not posting information about themselves that they wouldn't want employers colleagues, students, young people or parents to see
- Not retaliating to any incident
- Keeping evidence of any incident
- Promptly reporting any incident using existing routes for reporting concerns.

Staff in schools, as well as students, may become targets of cyberbullying. Staff should never retaliate to, i.e. personally engage with, cyberbullying incidents. They should report incidents appropriately and seek support.
Staff should report all incidents to the designated line manager or member of their school senior management team. The designated person will take responsibility for ensuring the person being bullied is supported, for investigating and managing the incident, and for contacting the police and Local Authority if appropriate.
For various reasons, staff may find it difficult to report to their line manager in the first instance. They may want additional support or advice. They should know they can seek advice and help from their Union, professional association, from Teacher Support Network, or other organisation

Further information and advice regarding cyber bullying can be found in the DfE guidance document Preventing and Tacking Bullying 2014.