E-Safety and Social Media Guidance
For School Based Staff

High Expectations
Caring
Positive Attitude
Successful

Policy reviewed: June 2019   To be reviewed: June 2021

High Expectations, Caring, Positive Attitudes
& Successful

STRENGTHS OF OUR SCHOOL

The Children
Are well behaved, calm and polite
Are engaged, positive and resilient
Are supportive and helpful towards others
Have an input on important decisions
Have a sense of belonging

The Community
School supports the whole family not just the child
Recognises the importance of attendance
Spreads our growing reputation as a good school
Helps celebrate the children's achievements
Supports the school on improving behaviour

The Curriculum
Is a fun curriculum that is engaging
Maintains a strong focus on the basic skills
Is enriched through extra-curricular activities
Supports our most vulnerable children
Provides a rich variety of experiences & opportunities

The Staff
Develop nurturing relationships with children
Provide good quality teaching and learning
Support one another to help the children
Are consistent in how they treat children
Identify children's SEN needs early

THE CURRICULUM WE HOPE TO PROVIDE

Skills
Fluent and confident in Reading, Writing and Maths
Communicate with confidence
ICT skills fit for the future
Life skills – money, time, cooking
Safety skills – Swimming, healthy choices
Problem-solving skills – Patience & Resilience

Attitudes
Confident and independent
The belief they can reach for the stars
Celebrate a range of cultures
Take responsibility for the environment
Be honest and learn from their mistakes
Children who are caring and helpful

Experiences
To have 1st hand experiences of…
Going away on a residential trip
Visiting a range of places of worship
A chance to look after an animal
Relevant trips to theatres/farms/beaches
Taking part in public performances
Work experiences & further education

Knowledge
High school ready English & maths
To know about local places of interest
To know where we are in the world
Life skills – money, time, cooking
Information about possible careers
To know major historical facts
To know their own strengths

E-Safety and Social Media Guidance

The guidance in this document is intended to allow everyone connected to **Hunslet Carr Primary School** a clear explanation of what is expected of them with regards to the safe use of the internet and appropriate use of Social Media.

CONTENTS

Section 1 – Overview
Section 2 – Responsibilities
Section 3 – Social Contact with Students, Children or Young People
Section 4 – Social Media
Section 5 – Inappropriate Material
Section 6 – Creating Images of Students through Photography & Video
Section 7 – Internet Use
Section 8 – Use of personal technology/equipment in School
Section 9 – Confidentiality and Security
Section 10 – Cyber Bullying

Section 1
Overview

Computing and the internet are essential tools for learning and communication that are used in **Hunslet Carr Primary School** to deliver the curriculum, and to support and challenge the varied learning needs of its students.

Computing is also used to share information and ideas with all sections of the school community through the school website and more recently our Twitter feed.

At **Hunslet Carr Primary School** 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, inciting hate through the promotion of extremist views, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. Staff have a duty of care to protect children from the risk of harm, as well as a duty to ensure their conduct does not bring into question their suitability to work with children.

This guidance takes into account the principles of the Safer Working Practice Guidance, as well as guidance from the Department for Education and CEOP (Child Exploitation and Online Protection). It also includes new regulations concerning the school's duty to Prevent children from accessing materials that might lead to inciting hate through the promotion of extremist views.

This guidance applies to all staff employed either directly or indirectly by **Hunslet Carr Primary School** as well as volunteers and staff not employed directly by the school but based at the school. 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 document, 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 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 **Hunslet Carr Primary School's** code of conduct (as set out in the Staff Handbook) 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 Safeguarding and Child Protection Policy and Procedures.

Staff are solely responsible for any content on their personal social media networks and electronic devices. Staff are responsible for managing their 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 bringing the school into disrespect

Staff are also responsible for ensuring their 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 with Students.
Staff must not establish or seek to establish social contact with students, for the purpose of securing or strengthening a friendship or 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. Staff should only contact students in school, using school equipment and regarding school matters, with appropriate permission from the Headteacher.

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 the prior consent of the Headteacher 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. 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.

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

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.

Section 5
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 a 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 is a range of offences about incitement of hatred by race, religion, sexual orientation and particular offences concerning harassing or threatening individuals which include 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, raising serious concerns about the suitability of the adult to continue to work with students.

Individuals also need to be mindful of actions outside the workplace 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
- accessing materials that can be used to incite hate through the promotion of extremist views
- 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 celebrating an achievement. However, written permission must be gained from legal guardians as well as the Headteacher before 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 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 workplace. **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 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 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 workplace 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 workplace 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.

Under the school's duty to Prevent extremist views under no circumstance should a member of staff use school equipment to research and view material that is likely to cause offence and incite hateful views.

Section 9
Confidentiality and Security

Members of staff may have access to confidential information about students and the organisation 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.

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. The 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 GDPR legislation. For further guidance about confidentiality issues and safe storage of data, please ask Hayley Stewart, the school's GDPR officer.

Section 10
Cyber Bullying

All forms of bullying, including cyberbullying, 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 workplace. 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 cyberbullying could be considered criminal offences under a range of different laws. Cyberbullying 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, websites, 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 & protect access to 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. use of a pin code.
- not posting information about themselves that they wouldn't want employers colleagues, students 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 cyberbullying can be found in the DfE guidance document Preventing and Tacking Bullying 2014.

- **Not knowing the schools policy and what each section means is not a reasonable defence for not following it**. It is at the back of the handbook and on the school website. If in doubt – ask!
- **It should not be possible either through your words, posts or photos to know that you work in a school.** While 99% of the people on the internet are safe and good-natured, there are people who will try and befriend you because, through you, they would have access to children.
- **No member of school staff should communicate with any child/parent, past or present from our school through social networking** including friends of friends – you need to make sure your settings are at the highest possible security.

- **School staff should not make any comment likely to cause an offence about children, families, the school or any other member of staff on a social networking site.** If you are unsure whether a comment will cause offence or not don't write it.
- **Ask non-school based friends to be very careful about what they Tag or Post about you.** You might have the highest settings and not post photos of yourself but if your friend posts a picture and tags you in you could find that children and parents have access.

Anecdotal evidence from Leeds HR is that over 50% of their disciplinary cases now concern the misuse of Social Media.