Elton Primary School & Nursery

Social Networking and Acceptable Use Policy

In our school, the wellbeing and education of all our children comes first

Full Governors	Summer 2022
Review	Summer 2024

Introduction to the Policy

The school is aware and acknowledges that increasing numbers of adults and children are using the internet and social networking sites. Those social networking sites with the widest use are Facebook, Twitter, Pinterest, Snapchat, Instagram and TikTok.

The widespread availability and use of internet and social networking applications bring opportunities to understand, engage and communicate with information and audiences in new ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with both safeguarding and our reputation.

This policy and associated guidance is to protect staff and advise school leadership on how to deal with potential inappropriate use of internet and social networking sites.

The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice.

Purpose

The purpose of this policy is to ensure:

- That the school is not exposed to legal risks,
- That the reputation of the school is not adversely affected,
- That every step is taken to ensure that staff, children and Governors are clearly protected from inappropriate material,
- That our users are able to clearly distinguish where information provided via social networking applications is legitimately representative of the school.

Internet Use:

Pupil access to the Internet

Pupils will be informed by staff of their rights and responsibilities as users through the pupil agreement and reinforcement during lessons. Pupils will not be allowed undirected use of the Internet. Staff will often provide pupils with links to sites which have been reviewed and evaluated prior to use. Staff must remain vigilant when their pupils are using the Internet in order to ensure that offensive or irrelevant materials are not accessed. As with printed materials, Parents and carers are ultimately responsible outside of school for setting and conveying the standards that their children should follow when using media and information sources. Individual users of the Internet in school are responsible for their own behaviour and communications over the Internet.

Pupil Guidelines for Computer Use

The Internet is provided for pupils to find information, practice skills and communicate with others. Access is a privilege, not a right and that access requires responsibility. Unauthorised use of the Internet or use of unauthorised websites will not be tolerated.

Individual users of the Internet are responsible for their behaviour and communications over the network. Users are expected to comply with school standards and to honour the agreements they have signed. During school, teachers will help guide pupils toward appropriate websites, outside of school, families bear responsibility for such guidance.

Staff may review files and communications stored in User Areas to ensure that users are using the system responsibly. Users should not expect that files stored on servers or drives would always be private.

Staff access to the Internet

School staff have access to the Internet for preparation of materials and the exchange of information for professional purposes. While personal use of the Internet in their own time is permitted, staff are not allowed to download any material in breach of copyright (or any other) law or of such a size as to take up an unreasonable amount of space on our servers. All users of the network must be aware that their user area, including their Internet use history, may be accessed by network administrators and files may be removed. (See Appendix A for the signed agreement of acceptable use for all adults).

School Procedures

Web Filtering

The school benefits from the filtering provided by Cheshire West and Cheshire. Elton Primary School and Nursery's learning platform also has a number of e-safety features including the ability to monitor all messages/emails sent by pupils and staff and a tracking system that shows actions of members of the website/learning platform. Any member of the school community can bring a website which causes them concern to the attention of the Computing Coordinator who can arrange for that site to be blocked in school by CWAC ICT Advisors.

School Rules

The school has developed a set of guidelines for Computer Use including the use of the Internet. These rules will be explained to all pupils, and kept under review. They are displayed on the screen of each of the computers.
All members of staff are responsible for explaining to pupils the rules and their implications. All members of staff need to be aware of possible misuses of on-line access and their responsibilities towards pupils.

Social Networking:

Facebook is targeted at older teenagers and adults. They have a 'no under 13' registration policy and recommend parental guidance for 13 to 16 year olds.

Twitter states that its service is not for children under the age of 13, therefore you should not be creating accounts within school specifically for children under this age to use independently.

Instagram and Snapchat have a minimum age of 13, in compliance with the Children's Online Privacy Protection Act.

This guidance is to advise and protect staff from accusations of improper relationships with pupils.

To register for Pinterest you need a Facebook or Twitter account – therefore this is not appropriate for children.

SCOPE

This policy covers the use of social networking applications by all school stakeholders, including, employees, Governors and pupils. These groups are referred to collectively as 'school representatives' for brevity.

The requirements of this policy apply to all uses of social networking applications which are used for any school related purpose and regardless of whether the School representatives are contributing in an official capacity to social networking applications provided by external organisations.

Social networking applications include, but are not limited to:
➢ Blogs, for example Blogger,

- ➢ Online discussion forums, such as netmums.com,
- ➢ Collaborative spaces, such as Facebook,
- ➢ Media sharing services, for example YouTube,
- ➢ 'Micro-blogging' applications, for example Twitter.

All school representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. **They must also operate in line with the School's Equality and Diversity Policy.**

Use of Social networking sites in work time

Use of social networking applications in work time for personal use only is not permitted, unless permission has been given by the Headteacher.

Social Networking as part of School Service

All proposals for using social networking applications as part of a school service (whether they are hosted by the school or by a third party) must be approved by the Headteacher first. Use of social networking applications which are not related to any school services (for example, contributing to a wiki provided by a professional association) does not need to be approved by the Headteacher. However, school representatives must still operate in line with the requirements set out within the policy

School representatives must adhere to the following Terms of Use. The Terms of Use below apply to all uses of social networking applications by all school representatives. This includes, but is not limited to, public facing applications such as open discussion forums and internally-facing uses such as project blogs regardless of whether they are hosted on school network or not.

Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct. Elton Primary School and Nursery expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Terms of Use
Social Networking applications

- Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns.
- Must not be used in an abusive, racially abusive, discriminatory or hateful manner
- Must not be used for actions that would put school representatives in breach of school codes of conduct or policies relating to staff.
- Must not breach the school's misconduct, equal opportunities or bullying and harassment policies.
- Must not be used to discuss or advise any matters relating to school matters, staff, pupils or parents.
- No staff member should have a pupil or former pupil under the age of 18 as a 'friend' to share information with.
- Employees should not identify themselves as a representative of the school
- References should not be made to any staff member, pupil, parent or school activity / event unless prior permission has been obtained and agreed with the Head Teacher
- Staff should be aware that if their out-of-work activity causes potential embarrassment for the employer or detrimentally effects the employer's reputation then the employer is entitled to take disciplinary action.
- School staff will not invite, accept or engage in communications with parents or children from the school community to any personal social networking sites while in employment at Elton Primary School.
- Any communication received from children to School Representatives must be immediately reported to the Head Teacher – Designated Child Protection Officer and procedures for safeguarding followed.

Violation of this policy will be considered as gross misconduct and can result in disciplinary action being taken against the employee up to and including termination of employment.

Guidance/protection for staff on using social networking
- No member of staff should interact with any pupil in the school on social networking sites
- No member of staff should interact with any ex-pupil in the school on social networking sites who is under the age of 18. This means that no member of the school staff should request access to a pupil's area on the social networking site. Neither should they permit the pupil access to the staff members' area e.g. by accepting them as a friend.
- Where family and friends have pupils in school and there are legitimate family links, please inform the Headteacher. However, it would not be appropriate to network during the working day on school equipment.
- It is illegal for an adult to network, giving their age and status as a child.
- If you have any evidence of pupils or adults using social networking sites in the working day, please contact the named Child Protection person in school.

Guidance/protection for Pupils on using social networking
- No pupil under 13 should be accessing social networking sites. This is the guidance from Twitter, Snapchat, Instagram, Pinterest, Facebook and MSN/SKYPE. There is a mechanism on Facebook where pupils can be reported via the Help screen; at the time of time of writing this policy the direct link for this is: http://www.facebook.com/help/contact.php?show_form=underage
- No pupil may access social networking sites during the school working day.
- Children are not allowed to bring mobile phones to school.
- No pupil should attempt to join a staff member's areas on networking sites. If pupils attempt to do this, the member of staff is to inform the Head teacher. Parents will be informed if this happens
- No school computers are to be used to access social networking sites at any time of day.
- Any attempts to breach firewalls will result in a ban from using school ICT equipment other than with close supervision.
- Please report any improper contact or cyber bullying to the class teacher in confidence as soon as it happens.

- We have a zero tolerance to cyber bullying.

Child protection guidance

If the Headteacher receives a disclosure that an adult employed by the school is using a social networking site in an inappropriate manner as detailed above they should:
- Record the disclosure in line with their child protection policy.
- Schools must refer the matter to the LADO (Local Area designated Officer) who will investigate via Cheshire Police Child Protection Team.
- If the disclosure has come from a parent, take normal steps to calm the parent and explain processes
- If disclosure comes from a member of staff, try to maintain confidentiality
- The LADO will advise whether the member of staff should be suspended pending investigation after contact with the police. It is not recommended that action is taken until advice has been sought and given.
- If disclosure is from a child, follow your normal process in your child protection policy until the police investigation has been carried out.

Cyber Bullying and Sexual Exploitation

Parents should be clearly aware of the school's policy of access to social; networking sites.
Where a disclosure of bullying is made, schools now have the duty to investigate and protect, even where the bullying originates outside the school.
This can be a complex area, and these examples might help:
- A child is receiving taunts on Facebook and text from an ex pupil who moved three months ago: This is not a school responsibility, though the school might contact the new school to broker a resolution.
- A child is receiving taunts from peers. It is all at weekends. The pupils are in the school: The school has a duty of care to investigate and work with the families, as they attend the school.
- A child is receiving taunts from peers. It is all at weekend using Facebook. The pupils are in Y5: This is the tricky one. The school has a duty of care to investigate and work with the families, as they attend the school. However, they are also fully within their rights to warn all the parents (including the victim) that they are condoning the use of Facebook outside the terms and conditions of the site and that they are expected to ensure that use of the site stops. At any further referral to the school the school could legitimately say that the victims and perpetrators had failed to follow the school's recommendation. They could then deal with residual bullying in the school, but refuse to deal with the social networking issues. Once disclosure is made, investigation will have to involve the families. This should be dealt with under the school's adopted anti bullying policy.
- If parent / carers refuse to engage and bullying continues, it can be referred to the police as harassment.
- A child receives an indecent image of another child or adult – this would be immediately referred to the iART team and police.
- A child is harassed for sending an indecent image of themselves to another child or adult- this would be immediately referred to the iART team and police.
- A child is asked for an indecent image of themselves by another child or adult – immediately referred to the iART team and the police.

This guidance can also apply to text and mobile phone cyber bullying.

Staff/Visitor/Governor signed agreement

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This procedure is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school e-safety coordinator. Any information created or held on our systems will not be considered private by default: this includes emails and other internet connections.

➢ I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
➢ I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities. I will ensure that my passwords comply with security arrangements by containing at least 8 characters with three of the following four requirements: capital letter, lower case letter, special character and number.
➢ I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
➢ I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
➢ I will not send or forward any emails which contain jokes, gossip or anything likely to cause offence. I am aware that by forwarding such emails I would be treated as if I created the email itself.
➢ I will only use the approved, email system(s) for any school business.
➢ I will not email or use services like drop box to share any sensitive or confidential information with ANYONE without permission from my manager.
➢ When forwarding emails I will judge whether it is necessary or appropriate to include all the thread.
➢ I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Any such data must be encrypted.
➢ I will not install any hardware of software without permission of **the Headteacher**
➢ I will not attach any personal device to the school system without permission.
➢ I will not use personal electronic equipment in school without permission from the Headteacher; and I understand that all of the requirements of this policy then applies to that device. Mobiles phones are allowed in the staffroom and around school outside of the normal children's hours of 8:45-3:15 so long as children are not present.
➢ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
➢ Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
➢ I understand that all my use of the Internet and other related technologies are monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
➢ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
➢ I will respect copyright and intellectual property rights.
➢ **I will ensure that my online activity, both in school and outside school, on the internet and all social networking sites will not bring my professional role or my employer into disrepute.**
➢ **I will not use social media or other internet services at any time in a way that is critical of my employment. I am aware that all my use of social media is covered by this.**
➢ I will not friend or follow children or their parents on any social network without the permission of the Head. I will not use personal mobile phones or emails to contact them without permission of the Head.
➢ I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
➢ I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature
I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …………………….………… Date ……………………

Full Name ……………………………….......................................(printed)

Job title . . . .