Uplands Primary School

Social Media Policy and Use of Mobile Phones and Digital Photography Policy

Date agreed: October 2022
Date for renewal: October 2023

Social Media:

Social media and social networking sites play an important role in the lives of many people. We recognise that sites bring risks, but equally there are many benefits to be reaped. This gives clarity to the way in which social media/mobile phones are to be used by pupils, social media/mobile phones are to be used by pupils, governors, visitors, parent helpers and school staff at Uplands Primary School. It will also provide guidance for parents. This policy reflects the guidelines in the Uplands Primary School Acceptable Use Policy (AUP), and should also be read in conjunction with other policies such as:

- County Council Guidance on using Social Media
- Online Safety Policy
- ICT Acceptable Use Policy for Staff
- Disciplinary Procedures
- Equalities Policy
- Child protection policy
- Safeguarding policy
- Behaviour and anti-bullying policies
- Staff code of conduct
- Remote and home learning policies.
- GDPR policy

The school will act within the guidance laid out in Keeping Children Safe in Education 2022 to ensure that the safety of our pupils is at the heart of all we do.

The risks presented by social media:
The school recognises the risks associated with use of the Internet and social media and regulates their use to ensure this does not damage the school, its staff and the people it serves.
Principal amongst these risks are:

- Cyber bullying by pupils/students;
- Access to inappropriate material;
- Offending behaviour toward staff members by other staff or pupils/students;
- Other misuse by staff including inappropriate personal use;
- Inappropriate behaviour, criticism and complaints from external sources;
- Threat of grooming/radicalisation from external sources;
- Loss or theft of personal data;
- Virus or other malware (malicious software) infection from infected sites;
- Disclosure of confidential information;
- Damage to the reputation of the school;
- Social engineering attacks - i.e. the act of manipulating people into disclosing confidential material or carrying out certain actions;

- Civil or criminal action relating to breaches of legislation;
- Staff members openly identifying themselves as school personnel and making disparaging remarks about the school and/or its policies, about other staff members, pupils or other people associated with the school.

Applying the Policy:

There are four key areas:
A. The use of social networking sites by pupils within school
B. Use of social networking by staff in a personal capacity
C. Comments posted by parents/carers
D. Dealing with incidents of online bullying

A. The use of social networking sites by pupils within school
The School's Acceptable Use Policy (AUP) outlines the rules for using computing equipment in school and these rules therefore apply to use of social networking sites. Pupils are not expected to be using social media sites within school. Such sites should not be used/accessed in school unless under the direction of a teacher and for a purpose clearly apparent from the learning objective of the relevant learning experience. If social media sites are used, then staff will carry out a risk assessment to determine which tools are appropriate.

In terms of private use of social networking sites by a child, it is generally understood that children under the age of 13 are not permitted to be registered, including Facebook and Instagram to name two. The school will not encourage children to have social media accounts, and will teach safe use of these through Computing and Online Safety lessons.

B. Use of social networking by staff in a personal capacity

Using the Internet and social media for approved school purposes
Staff must ensure that they use the Internet sensibly, responsibly and lawfully and that use of the Internet and social media does not compromise school information or computer systems and networks. They must ensure that their use will not adversely affect the school or its business, nor be damaging to the school's reputation and credibility or otherwise violate any school policies. In particular:

- The school's Internet connection is for business use and its use, and use of social networking, must only take place in line with the school's policies;
- When acting with approval on behalf of the school, under no circumstances may staff comment or contribute unless identifying themselves as school staff;
- Personal email or social media accounts must never be used to conduct school business. Any accounts created for this purpose must link to a school email address. The only exception is the use of professional networks (such as LinkedIn), where it is acceptable to use an account linked to a personal email address in both a professional and personal capacity;
- Staff members must report any safeguarding issues they become aware of;
- Staff members must not cite or reference pupils/students/parents without approval;
- Material published must not risk actions for defamation, or be of an illegal, sexual, discriminatory or offensive nature;
- Material published must be truthful, objective, legal, decent and honest;
- Material published must not breach copyright;

- Any publication must comply with all of the requirements of the General Data Protection Regulation (GDPR) 2018, and must not breach any common law duty of confidentiality, or any right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information;
- Material published must not be for party political purposes or specific campaigning which in whole or part appears to affect public support for a political party;
- Material published must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns;
- The tone of any publication must be respectful and professional at all times, and material must not be couched in an abusive, hateful, or otherwise disrespectful manner;
- Publication must be in line with school policies;
- If used with pupils/students, staff must ensure that the site's rules and regulations allow the age group to have accounts and that the parents are informed of its use;
- Staff members must not use the Internet or social media if doing so could pose a risk (e.g. financial or reputational) to the school, its staff or services or where they do not have the approval from the Senior Leadership Team.

Personal use of social media

It is possible that a high proportion of staff will have their own social networking site accounts. It is important for them to protect their professional reputation by ensuring that they use their personal accounts in an appropriate manner.

Guidelines are issued to staff:

- Staff **should** refrain from identifying themselves as working for the school in a way that could have the effect of bringing the school into disrepute
- Staff **must not** express a personal view as a school employee that the school would not want to be associated with
- Staff **must** notify the Senior Leadership Team immediately if they consider that content posted via any information and communications technology, including emails or social networking sites, conflicts with their role in the school
- Staff must **never** add pupils as 'friends' into their personal accounts (including past pupils under the age of 18).
- Staff are **strongly advised** not to add parents as 'friends' into their personal accounts. If this has happened; they **must not** engage in any discussion regarding the school whether expressing personal views or opinions or simply recounting events or stating facts.
- Staff **must not** post comments about the school, pupils, parents or colleagues including members of the Governing Body.
- Staff **must not** post information or opinions about Uplands Primary School or pictures of school events.
- Staff **must not** disclose any data or information about the school, colleagues in the school and/or partner organisations, pupils/students or parents that could breach the General Data Protection Regulation (GDPR) 2018
- Staff **must not** use the Internet or social media in or outside of work to bully or harass other staff or others (this includes situations when the intended victim is unaware of the abuse)
- Staff **must not** use social networking sites within lesson times (for personal use).

- Staff **should only** use social networking in a way that does not conflict with the current National Teacher's Standards or the school's AUP.
- Staff **should** review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality.
- Staff **should** read and comply with 'Guidance for Safer Working Practice for Adults Who Work with Children and Young People' and 'Keeping Children Safe in Education 2021'.
- Inappropriate use by staff should be referred to the Headteacher in the first instance and may lead to disciplinary action.

With the rise in identity theft and fraud, staff may wish to consider the amount of personal information that they display on personal profiles. School staff must never give out personal details of others, such as home address and telephone numbers. Staff must handle all personal or sensitive information in line with the school's Data Protection Policies.

C. Comments posted by parents/carers

Parents and carers will be made aware of their responsibilities regarding their use of social networking. Methods of school communication include the prospectus, the website, newsletters, school owned social media accounts, letters and verbal discussion. School policies (which will be made available on the School's website) and documents provide further information regarding appropriate channels of communication and means of resolving differences of opinion. Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for the child.

- Parents must not post pictures of pupils, other than their own children, on social networking sites where these photographs have been taken at a school event.
- Parents should make complaints through official school channels rather than posting them on social networking sites.
- Parents should not post malicious or fictitious comments on social networking sites about any member of the school community. This includes any comments, photos or posts that could be interpreted as derogatory in any way towards specific members of the school community or the school itself.
- School owned social media accounts will have commenting facilities turned off so this is not an available means of communication for parents.

D. Dealing with incidents of online bullying/inappropriate use of social networking sites:

Staff

The school will consider it a potential disciplinary matter if users utilise any information and communications technology, including email and social networking sites, in such a way as to bully/harass others in the school or in partner organisations, or pupils/students or parents, whether this takes place during or outside of work. Staff members need to be aware that no matter what the privacy settings on their social media/networking site, inappropriate/derogatory information about a colleague in the school or partner

organisations, pupils or parents, can find its way into the public domain even when not intended.

It should be noted that a person does not need to directly experience this form of victimisation in order for it to be classed as cyber bullying/harassment. The fact that a person is unaware that offensive or derogatory comments about them have been placed on websites still fits the criteria of cyber bullying/harassment.

If a staff member receives any threats, abuse or harassment from members of the public through their use of social media then they must report such incidents using the school's procedures.

Senior Leadership responsibility in relation to Bullying and Harassment

The school owes a duty to take reasonable steps to provide a safe working environment free from bullying and harassment. For this reason, it is essential that the Senior Leadership Team take appropriate steps to deal with any incident where it is alleged that a staff member has subjected others to abusive or personally offensive emails, phone calls or content on social networking sites such as Facebook, Twitter, or by any other means.

If a Senior Leader is made aware of such an allegation, the Senior Leadership Team should deal with it in the same way as any other incident of bullying or harassment in line with school policies, by investigating the allegations promptly and appropriately and providing the victim with appropriate support to demonstrate that the matter is being dealt with seriously.

Senior Leaders should encourage staff to preserve all evidence by not deleting emails, logging phone calls and taking screen-prints of websites. If the incident involves illegal content or contains threats of a physical or sexual nature, the Senior Leadership team should consider advising the employee that they should inform the police. In the event that such evidence contains indecent images of children, it is an offence to save, send, or alter an image or to show it to anyone else. Therefore, the evidence must be placed in a secure location such as a locked cupboard where others will not be able to see it. In these circumstances the Police should be contacted immediately for advice.

Pupils/Students:

The school's Anti-Bullying and Behaviour Policies set out the processes and sanctions regarding any type of bullying by a child on the school roll. If a case of bullying/risky behaviour has been witnessed by, or reported to, a member of school staff, they must act immediately, following the guidance of the school's Child Protection, Behaviour and Anti-Bullying policies. This policy applies to pupil behaviour both inside and outside of school.

Uplands Primary School will not tolerate any child to child abusive harassment via technology, sharing of indecent images or viewing/sharing of harmful content. The school will follow procedures in the child protection policy and guidance in KCSIE 2022 relating to child to child abuse in such cases. Sanctions as outlined in our behaviour policy will be applied as necessary and referrals to outside agencies such as children's services or the Police will also be made where necessary.

Parents:
In the case of inappropriate use of social networking by parents, the Governing Body will contact the parent asking them to remove such comments and seek redress through the appropriate channels such as the Complaints Policy and will send a letter. (Appendix 1)

The Governing Body understands that, "There are circumstances in which police involvement is appropriate. These include where postings have a racist element or where violence is threatened or encouraged." Furthermore, "Laws of defamation and privacy still apply to the web and it is unlawful for statements to be written…which:

- expose (*an individual*) to hatred, ridicule or contempt
- cause (*an individual*) to be shunned or avoided
- lower (*an individual's*) standing in the estimation of right-thinking members of society or
- disparage (*an individual in their*) business, trade, office or profession." (National Association of Headteachers)

Section 2: Use of Mobile Phones and Digital Photography Policy

Children in Years R to 4 are not permitted to have mobile phones in school. Pupils in year 5/6 may bring a phone to school as they are often walking home from school and more independent. Y5/6 pupils are not permitted to use or check phones during the school day. If a child brings a phone to school, they must have their parent's permission and hand it in to their class teacher. Parents wishing to pass on messages must contact the school office.

Children have their photographs taken to provide evidence of their achievements for their development records (The Early Years Foundation Stage).

Staff, visitors, volunteers and students are <u>not permitted</u> to use their own mobile phones to take or record any images of school children for their own records during the school day. Staff may only use their phones to text or make calls in school away from pupils. For example, after school or in the staffroom at breaktimes. Staff needing to take an urgent call during teaching time must inform the office and use the school phones.

Procedures

- Under the General Data Protection Regulation (GDPR) 2018 school must seek parental consent to take photographs and use video recorders. Photographs will be stored on the school network, which is password protected, until the relevant permissions expires, should this occur then all photographs will be shredded or deleted from the school network.
- The school's digital cameras must not leave the school setting (unless on an educational visit).
- Photographs are printed in the setting by staff and images are then removed from the camera memory.
- Photographs of children may be taken and used in accordance with parental consent obtained via the Multimedia Consent form.

- Often photographs may contain other children in the background.
- Events such as Sports Day, outings, Christmas and fundraising events may be recorded by video and photographs by staff and parent/carers but always in full view of all attending.
- Parents must not post photographs or video containing other children on social media websites. (See Policy above).
- Many mobile phones have inbuilt cameras so staff mobile phones must not be used to take pictures of children in our school. Mobile phones can only be used by staff in the staff room or in classrooms before/after school operating hours and never when pupils are present.
- Visitors may only use their phones in the foyer or outside the building and should be challenged if seen using a camera inappropriately or photographing children.
- The use of cameras and mobile phones are prohibited in toilets.
- Staff are asked not to make personal calls during their working hours (contact hours with children). However in urgent cases a call may be made or accepted if deemed necessary and by arrangement with the Headteacher.
- All school cameras and videos should be kept securely at all times and used with appropriate authority.

Appendix 1

Inappropriate Use of Social Networking Site

Dear Mr/Mrs……..

It has come to the attention of the Governing Body that inappropriate comments regarding the school/members of the school community have been made on a social networking site/app.

As these comments do not comply with the expectations set out in the school's Social Networking Policy you are respectfully asked to remove them from the website/app.

We would encourage you to enter into productive communication with the school in order to resolve any outstanding differences. The school has an 'open door' policy with regard to dealing with parental communication and there are also policies in place such as the Complaints Policy if required.

Yours sincerely,

Chair of Governing Body

Appendix 2:
Legal and Policy Framework – From: Manual of Personnel Practice; School Social Media Policy. Hampshire County Council.

The School is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the school are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional Codes of Conduct, including the following:

- Human Rights Act 1998
- Common law duty of confidentiality
- General Data Protection Regulation (GDPR) 2018, and
- Employment Practices Data Protection Code

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. pupil and employee records protected by the General Data Protection Regulation (GDPR) 2018
- Information divulged in the expectation of confidentiality
- School or County Council business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
- Politically sensitive information.

Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Acts 1952, 1996 and 2013
- Copyright, Designs and Patents Act 1988.
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Equality Act 2010

Appendix 3

Staff Declaration

I have read and understand the School Social Media Policy and understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal. I understand that, in certain circumstances, inappropriate use of Social Media may become a matter for police or social care investigations. I understand that if I need any clarification regarding my use of Social Media, I can seek such clarification from any member of the Senior Leadership Team.

SIGNED: …….

DATE: …….

PRINT NAME: ……