**Talavera Junior School**
**Social Media POLICY**

**Document Name: Social Media Policy**

**Latest Review:** November 2018

**Next Review Planned:** November 2020

**Signed:_____ (Policy Owner)**

**Print Name:_____**

**Review Date:_____**

**Signed:_____ (Governor Approval)**

**Print Name:_____**

**Approval Date:_____**

**Talavera Junior School**
**Social Media Policy**

## POLICY CHANGE HISTORY

| Version | Date | Status | Policy Owner | Governor Approval | Comment |
|---|---|---|---|---|---|
| 1.0 | | | SM/HB | LT | |
| 1.1 | 02/11/16 | Approved | LC | LT | Updated in line with Hampshire guidance |
| 1.2 | 05/02/19 | Approved | LC | SK | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**Social Media Policy**
**Professional Guidance and Policy on Social Networking**
**Pupil and Teacher Safeguarding**
***( to be read alongside Staff Acceptable Use of ICT Policy)***

As a general rule, you should exercise caution when it comes to communicating with pupils and former pupils using the internet or mobiles.

For example, you should only use official school email accounts or virtual learning platforms to talk to current pupils online so that any communication is logged.

You should also only communicate on school matters as personal communication could be considered inappropriate and in breach of your professional code of conduct.

As the boundaries between the online and offline worlds blur, however, your pupils or parents might try to include you in their "friends" list on their online social network or get hold of your personal email address or mobile number. This could be harmless but it's important that you keep a professional distance online, just as you would in the offline world, and not include them as "friends".

If you have a mobile with Bluetooth technology, you could be at risk of "Bluejacking" (where another Bluetooth user in your vicinity can send you a message without knowing your number) or "Bluesnarfing" (where another Bluetooth user can access your mobile and steal things like your contact list, emails, texts and photos).

Ultimately, email or phone communications between you and a pupil or parent that are deemed to fall outside of agreed school guidelines might lead to disciplinary action or a criminal investigation.

***Here are a few tips to help you stay in control:***

- Keep your personal email address, Instant Messenger ID, mobile number and social networking ID private and don't use them for communications with your pupils or parents.
- If your Bluetooth is not switched off by default, switch it off and set it to refuse connections when you are at work.
- If, despite your best efforts, your personal contact details fall into the wrong hands and a pupil makes contact with you, let a senior manager know immediately.
- If calls or texts to your mobile are persistent, let your mobile network provider know too so that they can investigate and take the appropriate action.
- If you receive anonymous emails, IMs or messages on your social networking profile that you think could be from a pupil or parent- or if you feel you are being harassed or bullied online - report it to a senior manager and contact your internet service or social networking provider so that they can investigate and take the appropriate action.

**Cyber-bullying: Guidance Document for Pupils and Parents**

**Do -**

- Keep your passwords confidential
- Ensure you familiarise yourself with the school's policy for acceptable use of technology, the internet and email.
- Avoid the use of social networking sites whilst at school.
- Ensure that you understand how any site you use operates and therefore the risks associated with using the site
- Consider carefully who you accept as friends on a social networking site
- Report to your line manager any incidents where a pupil has sought to become your friend through a social networking site
- Check what images and information is held about you online but undertaking periodic searches of social networking sites and using internet search engines
- Take care when publishing information about yourself and images of yourself on line – assume that anything you release will end up in the public domain

- Be aware that any off-duty inappropriate conduct, including publication of inappropriate images and material and inappropriate use of technology could lead to disciplinary action
- Take screen prints and retain text messages, emails or voice mail messages as evidence
- Follow school procedures for contacting parents and/or pupils
- Only contact pupils and/or parents via school based computer systems
- Keep your mobile phone secure at all times
- Use a school mobile phone where contact with parents and/or pupils has to be made via a mobile (eg during an educational visit off site)
- Erase any parent or pupil data that is stored on a school mobile phone after use
- Seek support from your manager, professional association/trade union, friend, employee support line as necessary
- Report all incidents of cyberbullying arising out of your employment to your line manager
- Report any specific incident on a Violent Incident Report (VIR) form as appropriate
- Provide a copy of the evidence with your line manager when you report it and further evidence if further incidents arise
- Seek to have offensive online material removed through contact with the site
- Report any threatening or intimidating behaviour to the police for them to investigate
- Support colleagues who are subject to cyberbullying

**DON'T**

- Allow any cyberbullying to continue by ignoring it and hoping it will go away
- Seek to return emails, telephone calls or messages or retaliate personally to the bullying
- Put information or images on-line, take information into school, or share them with colleagues, pupils or parents (either on site or off site) when the nature of the material may be controversial
- Accept friendship requests from pupils or parents
- Release your private e-mail address, private phone number or social networking site details to pupils and parents
- Use your mobile phone or personal e-mail address to contact parents and/or pupils
- Release electronically any personal information about pupils except when reporting to parents
- Pretend to be someone else when using electronic communication
- Take pictures of pupils with school equipment without parental permission
- Take pictures of pupils on your own equipment

**Data Protection Act**

Schools, Local Education Authorities (LAs), the Department for Education and Skills (DCSF - the government department which deals with education), the Qualifications and Curriculum Authority (QCA), Ofsted, and the Learning and Skills Council (LSC) all process information on pupils in order to run the education system, and in doing so have to comply with the Data Protection Act 1998. This means, among other things, that the data held about pupils must only be used for specific purposes allowed by law. We are therefore writing to tell you about the types of data held, why that data is held, and to whom it may be passed on.

The **school** holds information on pupils in order to support their teaching and learning, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the school as a whole is doing. This information includes contact details, National Curriculum assessment results, attendance information, characteristics such as ethnic group, special educational needs, and any relevant medical information. From time to time schools are required to pass on some of this data to LEAs, the DCSF and agencies such as QCA, Ofsted and LSC that are prescribed by law.

The **Local Education Authority** uses information about pupils to carry out specific functions for which it is responsible, such as the assessment of any special educational needs the pupil may have. It also uses the

information to derive statistics to inform decisions on (for example) the funding of schools, and to assess the performance of schools and set targets for them. The statistics are used in such a way that individual pupils cannot be identified from them.

**Ofsted** uses information about the progress and performance of pupils to help inspectors evaluate the work of schools, to assist schools in their self-evaluation, and as part of Ofsted's assessment of the effectiveness of education initiatives and policy. Inspection reports do not identify individual pupils.

The **Department for Education and Skills** (DCSF) uses information about pupils for research and statistical purposes, to inform, influence and improve education policy and to monitor the performance of the education service as a whole. The DCSF will feed back to LAs and schools information about their pupils for a variety of purposes that will include data checking exercises, use in self-evaluation analyses and where information is missing because it was not passed on by a former school. The DCSF will also provide Ofsted with pupil level data for use in school inspection. Where relevant, pupil information may also be shared with post 16 learning institutions to minimise the administrative burden on application for a course and to aid the preparation of learning plans.

Pupil information may be matched with other data sources that the Department holds in order to model and monitor pupils' educational progression; and to provide comprehensive information back to LAs and learning institutions to support their day to day business. The DCSF may also use contact details from these sources to obtain samples for statistical surveys: these surveys may be carried out by research agencies working under contract to the Department, and participation in such surveys is usually voluntary. The Department may also match data from these sources to data obtained from statistical surveys.

Pupil data may also be shared with other Government Departments and Agencies (including the Office for National Statistics) for statistical or research purposes only. In all these cases, the matching will require that individualised data is used in the processing operation, but that data will not be processed in such a way that it supports measures or decisions relating to particular individuals, or identifies individuals in any results. This data sharing will be approved and controlled by the Department's Chief Statistician.

The DCSF may also disclose individual pupil information to independent researchers into the educational achievements of pupils who have a legitimate need for it for their research, but each case will be determined on its merits and subject to the approval of the Department's Chief Statistician.

Pupils, as data subjects, have certain rights under the Data Protection Act, including a general right of access to personal data held on them. If you wish to access your personal data, or you wish your parents to do so on your behalf, then please contact the relevant organisation in writing:

Talavera Junior School, Gun Hill, Aldershot, Hampshire GU11 1RG

Ofsted's Data Protection Officer at Alexandra House, 33 Kingsway, London WC2B 6SE

LSC's Data Protection Officer at Cheylesmore House, Quinton Road, Coventry, Warwickshire CV1 2WT

The DCSF's Data Protection Officer at DCSF, Caxton House, Tothill Street, London, SW1H 9NA.

In order to fulfil their responsibilities under the Act the organisation may, before responding to this request, seek proof of the requestor's identity and any further information required to locate the information requested.

Separately from the Data Protection Act, regulations provide a pupil's parent (regardless of the age of the pupil) with the right to view, or to have a copy of, their child's educational record at the school. If you wish to exercise this right you should write to the school.

## Data Protection Policy

**School Compliance**

The terms of the 1998 Data Protection Act, and any subsequent relevant legislation, to ensure personal data is treated in a manner that is fair and lawful.

Advice and guidance supplied in the ***Data Protection Advice for Schools*** flyer and ***Data Protection Guidance for Schools*** booklet.

Information and guidance displayed on the Information Commissioner's website (***www.dataprotection.gov.uk***).

This policy should be used in conjunction with the school's ***Internet Use Policy***.

**Data Gathering**

All personal data relating to staff, pupils or other people with whom we have contact, whether held on computer or in paper files, are covered by the Act.

Only relevant personal data may be collected and the person from whom it is collected should be informed of the data's intended use and any possible disclosures of the information that may be made.

**Data Storage**

- Personal data will be stored in a secure and safe manner.
- Electronic data will be protected by standard password and firewall systems operated by the school.
- Computer workstations in administrative areas will be positioned so that they are not visible to casual observers waiting either in the office or at the reception hatch.
- Manual data will be stored where it not accessible to anyone who does not have a legitimate reason to view or process that data.
- Particular attention will be paid to the need for security of sensitive personal data.

**Data Checking**

The school will issue regular reminders to staff and parents to ensure that personal data held is up-to-date and accurate.

Any errors discovered would be rectified and, if the incorrect information has been disclosed to

**Data Disclosures**

Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given.

When requests to disclose personal data are received by telephone it is the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.

If a personal request is made for personal data to be disclosed it is again the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested.

Requests from parents or children for printed lists of the names of children in particular classes, which are frequently sought at Christmas, should be politely refused as permission would be needed from all the data subjects contained in the list. (Note: A suggestion that the child makes a list of names when all the pupils are present in class will resolve the problem.)

Personal data will not be used in newsletters, websites or other media without the consent of the data subject.

Routine consent issues will be incorporated into the school's pupil data gathering sheets, to avoid the need for frequent, similar requests for consent being made by the school.

Personal data will only be disclosed to Police Officers if they display a legitimate need to have access to specific personal data.

A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

**Subject Access Requests**

If the school receives a written request from a data subject to see any or all personal data that the school holds about them this should be treated as a Subject Access Request and the school will respond within the 40 day deadline.

Informal requests to view or have copies or personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the school will comply with its duty to respond within the 40 day time limit.

This policy will be included in the Policy File.

Data Protection statements will be included in the school prospectus and on any forms that are used to collect personal data.