RICHMOND PARK PRIMARY SCHOOL
YSGOL PARC WAUNDEW

SOCIAL NETWORKING AND E-SAFETY POLICY

Date of Policy	**June 2018**
Date to be Reviewed:	**June 2020**
Approved at Governor's Meeting Dated:	**21st June 2018**
Signed by Chair of Governors:	

CONTENTS

1. Introduction

2. Scope

3. Status

4. Principles

5. Safer Social Media Practice in Schools

6. Overview and expectations

7. Safer Online Behaviour

8. Protection of Personal Information

9. Communication between pupils / schools staff

10. Social Contact

11. Access to inappropriate images and internet usage

12. Cyberbullying

13.Guidance/protection for Pupils on using social networking

14. Potential and actual breaches of the Code of Conduct

15. Carmarthenshire County Council Guidance on the use of Social Networking Sites

1.0 Introduction
Social networking activities conducted online outside work, such as blogging (writing personal journals to publicly accessible internet pages), involvement in social networking sites such as Facebook, Myspace or Twitter and posting material, images or comments on sites such as You Tube can have a negative effect on an organisation's reputation or image. In addition, Richmond Park School has a firm commitment to safeguarding children in all aspects of its work.

Following a parent survey in 2012, many parents commented that the school needed to improve the way it shared and communicated information with parents/carers. For this reason it was decided that social media would be a positive avenue to explore. A Facebook and Twitter account were created with the target audience being current parents/carers and prospective parents/carers of the school. We aim to raise the profile of the school both with our current cohort of families and within the wider community. The school has also developed a Twitter account to share good practice within certain initiatives snd to share with families the learning of pupils.

For families who do not have access to technology at home, we aim to combat this issue by welcoming parents/carers into the school to discuss school issues with the relevant members of staff. Parents evenings will be held at least once a year and regular correspondence will go back to parents via text or email messages and also by school letters, leaflets, etc if parents do not have access to email via a smartphone. We also hold regular events where parents are invited into the school to share pupils' learning and / or develop their personal skills and awareness of using technology.

1.1 **Objectives**
This policy sets out Richmond Park School's policy on social networking. New technologies are an integral part of our lives and are powerful tools which open up teaching and learning opportunities for school staff in many ways. This document aims to:
• Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
• Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use.
• Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
• Support safer working practice
• Minimise the risk of misplaced or malicious allegations made against adults who work with pupils
• Reduce the incidence of positions of trust being abused or misused

1.2 Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff will always advise the Headteacher of the justification for any such action already taken or proposed.

1.3 This policy takes account of employment legislation and best practice guidelines in relation to social networking in addition to the legal obligations of governing bodies.

2.0 Scope
2.1 This document applies to all staff who work in Richmond Park School as adopted by the governing body. This includes teachers, therapists, support staff, supply staff, administration staff, site staff, governors, volunteers and contractors.

2.2 It should be followed by any adult whose work brings them into contact with pupils. References to staff should be taken to apply to all the above groups of people in schools. Reference to pupils means all pupils at the school including those under the age of 18.

2.3 This policy should not be used to address issues where other policies and procedures exist to deal with them.

3.0 Status
3.1 This document does not replace or take priority over advice given by Carmarthenshire County Council, the safeguarding unit or the school's codes of conduct, dealing with allegations of abuse, but is intended to both supplement and complement any such documents.

4.0 Principles
4.1 Adults who work with pupils are responsible for their own actions and behaviour and should avoid any conduct which would lead any reasonable person to question their motivation and intentions.

4.2 Staff in schools should work and be seen to work, in an open and transparent way.

4.3 Staff in schools should continually monitor and review their practice in terms of the continually evolving world of social networking and ensure they follow the guidance contained in this document.

5:0 Safer Social Media Practice in Schools
5.1 **What is social media?**
For the purpose of this policy, social media is the term commonly used for websites which allow people to interact with each other in some way – by sharing information, opinions, knowledge and interests. Social networking websites such as Facebook, Twitter and MySpace are perhaps the most well known examples of social media but the term also covers other web based services such as blogs, video and audio podcasts, wikis, message boards, photo document and video sharing websites such as YouTube and micro blogging services such as Twitter. This definition of social media is not exhaustive as technology develops with new ways of communicating advancing every day.

5.2 For the purpose of this document the terminology Social Media is not exhaustive and also applies to the use of communication technologies such as mobile phones, cameras or other handheld devices and any other emerging forms of communications technologies.

5.3 The decision on using Social Media tools such as Facebook and Twitter (all school accounts) for school purposes has been made as a school and has the full support and backing of the Senior Leadership Team and Governing Body.

5.4 The school is aware of their responsibility to moderate any content and to ensure that the service is kept up to date. The tools must also be used in accordance with the school's

behaviour and complaints policies. The school uses the Meraki system to monitor and track school hardware, e.g. IPads, MacBooks, etc. This system also enables restrictions to prevent teachers/students from adding/deleting apps, making in-app purchases, etc. The school also uses the VPP system to purchase and allocate apps on teachers' IPads. No teachers should have access to either of these passwords or software. Only the Headteacher and Deputy Headteacher have access to these accounts.

5.5 It is important that the school is aware of how Social Media sites function and is aware how to make them as safe as possible. To improve communication between the home and school, parents are able to send direct messages to the school via our Facebook account. The Headteacher and Deputy Headteacher are the only members of staff with access to this account and are the only ones permitted to respond to parents/carers. Also, the Facebook page has the minimum age of followers set to 18+ to ensure that no children are able to comment on the school page.

5.6 In order to protect staff, a school approved email address has been used to set up our accounts on Twitter and Facebook. Therefore, no personal staff contact details or information can be shared with parents/carers, etc.

5.7 The school uses Facebook and Twitter primarily to develop communication links between parents/carers and prospective parents/carers of the school, as well as share examples of good practice on a daily basis. For this purpose, the Headteacher and Deputy Headteacher have sole rights when creating the posts on Facebook. If other teachers/staff would like to inform parents/carers of information via Facebook, they must pass the required information on to the Headteacher or Deputy Headteacher to post the information for them.

5.8 All members of teaching staff have been provided with an IPad for teaching and learning purposes. Under the terms of the Acceptable Use Policy, the IPad is allowed to be taken home for the purpose of lesson planning, etc.

5.9 All members of teaching staff have been provided with the password for the main school Twitter account (@RichmondParkCPS). They are encouraged to post 'tweets' which highlight examples of good practice from their own classes. They should only do this from their school device - not their personal device. Passwords should remain confidential amongst teaching staff and should not be shared with anyone else. Any images of children posted must have consent from the parent/carer.

6.0 Overview and expectations

6.1 All adults working with pupils have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of pupils. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, pupils or students, public in general and all those with whom they work. Adults in contact with pupils should therefore understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting.

6.2 The guidance contained in this policy is an attempt to identify what behaviours are expected of schools' staff who work with pupils. Anyone whose practice deviates from this document, the Acceptable Use policy (found in the staff handbook) and/or their professional or employment-related code of conduct may bring into question their

suitability to work with children and young people and may result in disciplinary action being taken against them.

6.3 School staff should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others. They should report and record any incident with this potential.

6.4 Safeguarding children is a key responsibility of all members of staff and it is essential that everyone at Richmond Park School considers this and acts responsibly if they are using social networking sites out of school. Anyone working in the school either as a paid employee or volunteer must not communicate with children via social networking.

7.0 Safer online behaviour

7.1 Managing personal information (e.g. having a strong password for different accounts, ensuring high privacy settings on personal accounts, etc) effectively makes it far less likely that information will be misused.

7.2 In their own interests, staff need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers. This will avoid the potential for pupils or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties.

7.3 All staff, particularly new staff, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and the school if they are published outside of the site.

7.4 Staff should never 'friend' a pupil at the school where they are working onto their social networking site. It would also be preferable that staff do not 'friend' parents of pupils either though it is recognised that staff and parents sometimes have friendships that precede employability at the school.

7.5 Staff should never use or access social networking sites of pupils and should never accept an invitation to 'friend' a pupil. Staff should neither accept an invitation or send an invitation of friendship with an ex-pupil who is below the age of 18.

7.6 Confidentiality needs to be considered at all times. Social networking sites have the potential to discuss inappropriate information and employees need to ensure that they do not put any confidential information on their site about themselves, their employer, their colleagues, pupils or members of the public.

7.7 Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the school, or another school, or Carmarthenshire County Council could result in formal action being taken against them. This includes the uploading of photographs which might put the school into disrepute.

7.8 Staff are also reminded that they must comply with the requirements of equalities legislation in their on-line communications.

7.9 Staff must never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring the school or Carmarthenshire County Council into disrepute.

The following is not permitted:

- The use of the school's name, logo, or any other published material without written prior permission from the Headteacher should be avoided. This applies to any published material including the internet or written documentation.

- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.

- The posting of any images of employees, children, governors or anyone directly connected with the school whilst engaged in school activities.

In addition to the above everyone at Richmond Park School must ensure that they:

- Do not make any derogatory, defamatory, rude, threatening or inappropriate comments about the school, or anyone at or connected with the school.

- Use social networking sites responsibly and ensure that neither their personal/professional reputation, or the school's reputation is compromised by inappropriate postings.

- Are aware of the potential of on-line identity fraud and to be cautious when giving out personal information about themselves which may compromise their personal safety and security.

8.0 Protection of personal information

8.1 Staff should ensure that they do not use school ICT equipment for personal use, e.g. camera or computers. All staff have access to a school IPad and laptop, but these should be used for work purposes only.

8.2 Staff should keep their personal phone numbers private and not use their own mobile phones to contact pupils or parents unless agreed with the Headteacher.

8.3 Staff should never share their work log-ins or passwords with other people.

8.4 Staff should not give their personal e-mail addresses to pupils or parents unless agreed with the Headteacher. Where there is a need for communication to be sent electronically the school e-mail address should be used. Likewise all telephone messages and conversations should take place on the school phone system.

8.5 Staff should keep their phone secure whilst on school premises. All mobile phones should be switched off whilst staff are on duty – other than in exceptional circumstances which have been discussed and agreed with a member of the senior leadership team.

8.6 Staff are advised to understand who is allowed to view the content on the pages of the sites they use and how to restrict access to certain groups of people.

9.0 Communication between pupils / schools staff

9.1 Communication between pupils and staff, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs.

9.2 Staff should not give their personal contact details, mobile numbers or personal e-mail addresses to pupils or parents.

9.3 Staff should not request, or respond to, any personal information from a pupil, other than that which might be appropriate as part of their professional role.

9.4 Staff should ensure that all communications are transparent and open to scrutiny. They should also be careful in their communications with pupils so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as 'grooming' in the context of sexual offending.

9.5 E-mail or text communications between an adult and a pupil outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites. Internal e-mail systems should only be used for work purposes.

10.0 Social contact

10.1 Staff should not establish or seek to establish social contact via social media / other communication technologies with pupils.

10.2 There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher are part of the same social circle, staff are transport escorts or a staff member provides respite. These contacts however, will be easily recognised and openly acknowledged. The school will organise staffing where possible so that staff who have such contact with pupils outside school do not work within the same class as the pupil. Staff have a responsibility to make any such contact known to the senior leadership team.

10.3 There must be awareness on the part of those working with pupils that some social networking contacts, especially where these are not common knowledge, can be misconstrued as being part of a grooming process. This can also apply to social networking contacts made through outside interests or through the staff member's own family.

11.0 Access to inappropriate images and internet usage

11.1 There are no circumstances that will justify adults possessing indecent images of children or adults on school devices. Staff who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing

indecent images of children is illegal. This will lead to criminal investigation and the individual being barred from working with children, if proven guilty.

11.2 Adults should ensure that pupils are not exposed to any inappropriate images or web links. Schools and schools' staff need to ensure that internet equipment used by pupils have the appropriate controls with regards to access e.g. personal passwords should be kept confidential. We use a website filtering tool provided by Carmarthenshire County Council to minimise any risk of exposure to inappropriate material to children.

11.3 Where indecent images of children are found by staff, the Headteacher/Child Protection Officer should be immediately informed. If the incident relates to the Headteacher, then the Deputy Child Protection Officer or Governor in charge of Child Protection should be informed. Schools should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

11.4 Where other unsuitable material is found, which may not be illegal but which raises concerns about that member of staff, the Headteacher/Child Protection Officer should be informed and advice sought. If the incident relates to the Headteacher, then the Deputy Child Protection Officer or Governor in charge of Child Protection should be informed. The school should not attempt to investigate or evaluate the material themselves until such advice is received.

12.0 Cyberbullying

12.1 Cyberbullying can be defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.'

12.2 Prevention activities are key to ensuring that staff and children are protected from the potential threat of cyberbullying. All employees are reminded of the need to protect themselves from the potential threat of cyberbullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.

12.3 If cyberbullying does take place, employees and children should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e-mails. Employees are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site.

12.4 Staff may wish to seek the support of their trade union or professional association representatives or another colleague to support them through the process.

12.5 Staff are encouraged to report all incidents of cyberbullying to their line manager or the headteacher. If the incident relates to the Headteacher, then the Deputy Child Protection Officer or Governor in charge of Child Protection should be informed. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police.

12.6 Children receive e-safety lessons as a regular part of their lessons and through visits by the schools' police liaison officer. E-Safety is the responsibility of all staff. The school also engages in Safer Internet Day each year.

12.7 Children are encouraged to report all incidents of cyberbullying to their teacher, a member of staff, their parents, etc. Children are also encouraged to report incidents of online abuse, cyberbullying, receiving inappropriate images, etc to CEOP (the link is on the bottom of the school website and HWB+ website). All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident.

13.0 Guidance/protection for Pupils on using social networking

13.1 No pupil under 13 should be accessing social networking sites. This is the guidance from both Facebook and MSN. 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

13.2No pupil may access personal social networking sites during the school working day.

13.3 All mobile phones must be handed into the children's class teachers at the beginning of the school day and the Internet capability must be switched off. Failure to follow this guidance could result in a total ban for the student bringing a mobile phone. Teachers should lock phones away securely or hand in to the school office for safekeeping.

13.4 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

13.5 No school computers are to be used to access social networking sites at any time of day. Staff are only permitted to access these sites via their own devices during their break/lunchtimes.

13.6 Children are advised to report any improper contact or cyber bullying to the class teacher in confidence as soon as it happens.

14.0 **Potential and Actual Breaches of the Code of Conduct**

In instances where there has been a breach of the above Code of Conduct, the following will apply:

14.1 Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the Disciplinary Procedure. A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the school's ethos and principles.

14.2 The Governing Body will take appropriate action in order to protect the school's reputation and that of its staff, parents, governors, children and anyone else directly linked to the school.

15.0 **Carmarthenshire County Council Guidance on the Use of Social Networking Sites**

Carmarthenshire County Council is aware that employees will use the internet to access social networking sites and other such facilities for personal purposes. Many employees are likely to participate in social networking on websites such as Facebook, My Space and Twitter as well as use Blogs to share views and opinions.

It is acknowledged that such sites are increasingly useful communication tools and are a part of modern life. However it is acknowledged that, following a number of recent incidences publicised within the media, there is the potential for such sites to blur the boundaries between personal and employment lives. Therefore, it is important that all employees are mindful that, when using such sites, they must consider the potential impact of their actions on their contract of employment with the Council.

Employees must remember that anything posted on a social networking site is in the public domain and reflects on the individual as an employee of the Authority. Consequently it is considered necessary to issue the following guidance to staff:

EMPLOYEES **MUST NOT USE** SOCIAL NETWORKING SITES:

- To breach confidentiality
- To criticise or abuse users of the Authority's services, any other Council employee or elected members
- To bring the Authority or any of its employees and/or its elected members into disrepute
- During working hours

FURTHERMORE ALL EMPLOYEES **MUST** ABIDE BY:

- Council Policies and Procedure (e.g. Internet Usage and Monitoring Policy, Flexitime Scheme)
- Codes of Practice (e.g. Data Protection Act 1998)
- Contract of Employment – Confidentiality clause
- Code of Conduct for Council Employees

Employees are advised that the publishing of any inappropriate, inaccurate or defamatory information/ material in the public domain may result in disciplinary action being taken by the Council in accordance with its Disciplinary Policy & Procedure. Furthermore, in certain circumstances, civil court proceedings could ensue.

Staff are reminded that the Council has a number of policies and procedures to enable staff to pursue personal concerns or grievances.
These include:-

- Grievance Policy & Procedure
- Dignity at Work Policy & Procedure
- Whistleblowing Policy & Procedure

Further information in respect of these Policies is available via the documents library on HwB Sharepoint.
Should you need any support or guidance in respect to these sites please contact your supervisor/line manager or contact the Human Resources Team.

Use of Social Media Guidance August 2011 People Management & Performance