Test Valley School

Social Networking Policy for Pupils

Rights Respecting Schools:	
Article 16:	Every child has the right to privacy. The law should protect the child's private, family and home life.
Article 17:	Every child has the right to reliable information from the media. This should be information that children can understand. Governments must help protect children from materials that could harm them.
Article 29:	Education must develop every child's personality, talents and abilities to the full. It must encourage the child's respect for human rights, as well as respect for their parents, their own and other cultures, and the environment.

Rationale

The widespread availability and use of social media applications bring opportunities to understand, engage, share information and communicate in new and exciting ways. It is important that our pupils are able to use these technologies and services effectively and flexibly. However, it is also important to ensure we balance this with our duties to our school, the community, our legal responsibilities and our reputation because social networking brings some dangers. Therefore, we must take steps to protect those who use social networking applications as it has implications for our duty to safeguard our pupils and staff.

Test Valley School is committed to ensuring that all pupils, staff and governors are aware of their responsibilities in connection with the growing use of social networking sites. It recognises that the use of such sites has become a very significant part of life for most pupils. They provide a positive way to keep in touch with friends and family, and can be used to exchange ideas and thoughts on common interests.

This Social Networking Policy aims to support innovation and provide a framework of good practice. It applies to all pupils at the school.

Principles

What is a social networking site?

'A social network service focuses on building online communities of people who share interests and/or activities, or who are interested in exploring the interests and activities of others. Many social network services are web-based and provide a variety of ways for users to interact, such as email and instant messaging services.'

Any site that allows the interaction between people and/or organisations can be considered social networking. Examples include Facebook, Instagram, Ask .FM, Snapchat, YouTube, Xbox Live and virtual worlds (such as Second Life, World of Warcraft, Fornite, Roblox).

Interacting with each other online is no different than interacting face-to-face: pupils need to be able to maintain the principles of respect, dignity, care, concern for and protection of others, and for safety in all interactions. Activities which are inappropriate, unethical, illegal, or which cause undue discomfort for members of the school community (including pupils, employees, parents, or others) should be avoided. Pupils who participate in online interactions must remember that their posts may reflect on the entire school community and, as such, may be subject to the same standards set out in the Behaviour Policy.

It is important to protect everyone at the school from allegations and misinterpretations which can arise from the use of social networking sites. Therefore, pupils need to be made aware that they have a responsibility to ensure that they protect the reputation of the school, and treat others with respect.

Safeguarding pupils is a key responsibility of all members of staff and it is essential that pupils are taught how to use social networking sites safely and securely. It is also important that pupils are aware of the risks associated with the inappropriate use of social networking sites.

Practice

A planned e-safety curriculum will be provided as part of Computing / PSHE / other lessons and will be regularly revisited by IT staff, Senior Leadership Team and the Governing Body.

Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities. Pupils will be taught in lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

Pupils will be made aware that for their personal security, all communication via social networking sites should be made with the awareness that anything said, shown or received could be made available, intentionally or otherwise, to an audience wider than that originally intended. It is therefore considered necessary that pupils are made aware of the following:

1. Due to the fact that social media sites are increasingly inter-connected, pupils should be aware that any content posted online may eventually (or immediately) show up on other sites and could continue to be available indefinitely. It is often very difficult or impossible to completely remove content once published. Not posting inappropriate content in the first place is the only way to completely protect against this possibility.

2. They must learn not to post anything they wouldn't want friends, parents, teachers, or a future employer to see, as they can’t control posted data once it is on the web.

3. Chats, conversations, and other messages that they believe to be private can be compromised, screenshots taken and shared with other users, or forwarded to people outside of friendship groups. This could then lead to more serious consequences if they do not know who they are communicating with.

4. Pupils need to be made aware that they should never send pictures of themselves that could be considered ‘indecent’ (partially or totally naked) as these images once sent cannot

ever be ‘unsent’ and do cause both the sender and receiver to commit potential criminal offences.

5. Pupils need to follow the school's classroom rules and expectations set out in the Behaviour Policy when writing online whilst at school or using school systems. It is acceptable to disagree with someone else's opinions; however, pupils need to do it in a respectful way and make sure that criticism is constructive and not hurtful.

6. When linking to other websites to support their thoughts and ideas, pupils need to be careful that they are linking to content that is appropriate and does not reflect poorly on themselves or the school community. It is important to be aware that the content accessed through a link could change at any time in the future.

7. How pupils represent themselves online is an extension of themselves. They must learn not to misrepresent themselves by using someone else's identity.

8. In order to be eligible to sign up for Facebook and many other services, they must know that they need to be at least 13 years old. They should know that they should not manage an account with a social media service if they are under 13 years as they are particularly vulnerable to becoming a victim of crime, and this is often against the terms of service.

9. Pupils need to be made aware that use of the school’s name, logo or other intellectual property (documents produced by the school) may not be published without first obtaining permission from the school.

10. Pupils need to know that the use of social media (Facebook, Twitter, etc.) is not permitted during school time unless specifically authorised by the teacher and controlled for learning purposes.

Pupils are also expected to abide by the following:

- To protect the privacy of Test Valley School, pupils may not, under any circumstances, create digital video recordings, record audio or take photographs of Test Valley School community members either at school or whilst attending Test Valley’s activities outside of school premises for online publication or distribution without prior permission from the school.
- Pupils may not use social media sites to publish unpleasant or harassing remarks about Test Valley’s school community members or post anything that could potentially bring the school into disrepute.
- Pupils who choose to post editorial content or photographs to websites or other forms of online social media (including their own personal social media sites) must ensure that their submission does not reflect poorly upon either the school or its members.

To ensure Privacy:

1. Pupils need to know how to exercise care with privacy settings and personal profile content, to ensure that posted content does not reflect poorly on themselves or the school in any

way or otherwise create a conflict of interest. Content should be placed thoughtfully and reviewed from time to time.

2. On most sites, pupils need to know that privacy settings can be changed at any time to limit access to profiles and search visibility, and that these changes should be made when necessary. However, pupils should remember that once something has been published there is no guarantee it can be completely removed.

3. To make it difficult for others to access information about a pupil's private life, they must make certain that their personal social networking profile is set to "private" and that personal information is not available to "friends of friends".

4. To be safe online, pupils need to know that they must never publish widely or publicly personal information, including, but not limited to, last names, phone numbers, addresses, exact birth dates, and pictures.

5. Pupils must always respect the privacy of others.

6. Pupils need to present their own work and never use other people's intellectual property without their permission. They need to know that it is a violation of copyright law to copy and paste other's thoughts. When paraphrasing someone else's idea(s), they must be sure to cite the source with the URL.

7. Pupils need to be made aware that pictures may also be protected under copyright laws so might need to verify they have permission to use the image by asking the teacher or IT Technician.

Pupils will receive education about the safe use of social networking sites from IT staff, their Computing Teacher, during PSHE lessons, from staff allowing access to the internet for learning purposes and school assemblies.

For additional guidance on where help might be available to support the pupil though any traumatic consequences, please see *Additional Resources* below.

School Facilities

Pupils must not access social networking sites for personal use via school information systems or by the use of school equipment.

Breaches of this Policy

Test Valley School does not discourage pupils from using social networking sites in an appropriate manner. However, the school will take seriously any occasions where the services are used inappropriately. If occasions arise where pupil actions could be deemed to be online bullying or harassment, these will be dealt with in the same way as other such instances and in accordance with the Anti-Bullying and Behaviour Policies.

Sanctions for use in the case of violation of the policy:

Any breach of this policy may lead to disciplinary action being taken against the pupil(s) involved. The full range of sanctions that are available to the school may be used in dealing with pupils who have breached the Social Networking Policy Regulations as stated above.

The specific disciplinary sanction imposed will depend on the seriousness of the incident and will be more severe for repeated offences.

The following school sanctions exist:

- Admonishment and counselling - for instance for those who might have been involved naively, unwittingly or at a low level.
- Prohibition from using the school Internet or other IT facilities for a period of time, where this might be an appropriate sanction for the offence committed and for safeguarding purposes.
- Confiscation of mobile devices until the end of the day or, in exceptional circumstances, parents asked to collect the device.
- Periods of break or lunchtime detention.
- Given that any breach of the Social Networking Policy regulations can have a seriously detrimental effect on the individual/s involved, extending to their professional reputation and that of the school, it should be recognised that depending on the seriousness of the allegations, action may be taken which could culminate in the pupil being excluded from the school for either a fixed period of time or permanently.
- There may be instances where the school will be obliged to inform the police of any activity or behaviour for which there are concerns as to its legality as a variety of offences (such as harassment, abuse, racism, slander, character defamation) may fall within the definitions of being offences.

Under the Regulation of Investigatory Powers Act 2000 (RIPA), the Head Teacher can exercise their right to monitor the use of the school's information systems and internet access where it is believed unauthorised use by pupils may be taking place; to ensure compliance with regulatory practices; to ensure standards of service are maintained; to prevent or detect crime, to protect the communication system and to pick up messages when someone is away from school.

Parents of pupils who are causing serious concerns should be kept informed at all times.

Roles and Responsibilities

Staff

- All staff will be familiar with this policy and guidelines.
- Tutors will ensure that pupils understand the policy and their own responsibilities as they arrive at the school.
- Teachers will provide opportunities for pupils to learn about the risks of the use of social networking sites and the possible implications of any inappropriate use of them.

- In lessons where internet use is pre-planned, it will be best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people are using.
- All staff will act as good role models in their use of social media and internet sites.
- Staff will instigate sanctions where appropriate and seek advice where necessary on the approach to be adopted if they are made aware of any potential issue.
- Pupils with 3G/4G phones may be able to access the internet on site. These internet connections are not on the school network and are therefore not filtered or monitored by the school.

SLT will:

- Be familiar with this policy and guidelines.
- Ensure that all pupils have access to what is contained in this policy and that new pupils are made aware of it.

Pupils will:

- Behave responsibly at all times in connection with the use of social networking sites.
- Co-operate with the school in ensuring the implementation of this policy.

The Governing Body will:

- Be familiar with this policy and guidelines.
- Monitor that all pupils have access to what is contained in this policy and that new pupils are made aware of it.

Links to other documents:

This policy is intended to ensure the rights of individuals to use social networking and their responsibilities to do so in a responsible manner as outlined in the following:

Libel Act 1843
Human Rights Act 1998;
Data Protection Act 1998;
Protection from Harassment Act
Freedom of Information Act 2000
Computer Misuse Act 1990, amended by the Police and Justice Act 2006;

Regulation of Investigatory Powers Act 2000 (RIPA)
Safeguarding Vulnerable Groups Act 2006
Keeping Children Safe in Education 2016

Additional Resources

- NSPCC Website — www.nspcc.org.uk
- BBC Webwise — www.bbc.co.uk/webwise
- Safety Net Kids — www.safetynetkids.org.uk/
- CEOP Command — www.ceop.police.uk
- SWGfL Facebook Checklist — http://www.swgflstore.com/products/facebook-check
- SWGfL eSafety Resources — http://swgfl.org.uk/products-services/esafety/resources

APPENDIX A

Pupils — Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head Faculty / Head of Year / other	Refer to Headteacher	Possible Referral to Police	Refer to IT Services for action re filtering / security etc.	Inform parents / carers	Restrict internet/network access or removal of device	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see guidance in above text)		X	X	X	X	?	X		X
Unauthorised use of non-educational sites during lessons	X				X		?	X	
Unauthorised use of mobile phone / digital camera / other mobile device	X						X	X	X
Unauthorised use of social media / messaging apps / personal email	X				X		X	X	X
Unauthorised downloading or uploading of files	X				X		X		X
Allowing others to access school network by sharing username and passwords	X				X		X		X
Attempting to access or accessing the school network using another pupil's account	X				X		X		X
Attempting to access or accessing the school network using the account of a member of staff	X	X	X	X	X	X	X		X
Corrupting or destroying the data of other users	X	X			X	?	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X			X	X	X		X
Continued infringements of the above, following previous warnings or sanctions	X	X			X	X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X	X	X	X	X		X
Using proxy sites or other means to subvert the school's filtering system		X		?	X		X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X				X	?	?		X
Deliberately accessing or trying to access offensive or pornographic material	X	X	?	X	X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X				X	X	X		?

NOTE: ? = means will be considered for action