USE OF SOCIAL MEDIA BY COLLEAGUES

Policy & Procedure No.	**HR02**
Reviewed & Updated:	**November 2019**
Next Review:	**November 2020**

CONTENTS

Reference to

LE01 Data Protection
LE02 Confidentiality
IT01 IT Security
Safeguarding Vulnerable Groups Act 2006

1. School Resource

School networked resources, including any provided Wi-Fi and remote access facilities, are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. This policy applies to all colleagues, consultants, contractors, temporary and other workers within Seadown School.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access; monitoring and / or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter which in turn could lead to the termination of employment.

2. The Internet, Mobile Phones & Social Media

The school is aware and acknowledges that increasing numbers of adults and children are using mobile phone and social networking sites. Some common examples are Facebook, Twitter and SnapChat. This policy and associated guidance are to protect staff and advise school leadership on how to deal with potential inappropriate use of social networking.

The widespread availability and use of social networking applications bring opportunities to understand, engage and communicate with audiences in new ways. It is important that we can use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our reputation. For example, if you make a comment about the school or County Council anywhere online, both in and out of school, you must state that it is an expression of your own personal view.

Our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.

The policy requirements in this document aim to ensure that;

- the school is not exposed to legal risks.
- the reputation of the school is not adversely affected.
- our users can clearly distinguish where information provided via social networking applications is legitimately representative of the school.
- provide this balance to support innovation whilst providing a framework of good practice.

This policy covers the use of social networking applications by all school stakeholders, including, employees, Governing Body 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, GDPR 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 applications in work time, for personal use only, is not permitted unless permission has been given by the Head teacher.

- Social Networking is already provided as part of Seadown School's Service and is monitored and provided by senior leadership and / or authorised technicians.

- 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.

3. Conditions of Use

3.1 Personal Responsibility

Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network to the Headteacher or, in their absence, the Deputy Head.

3.2 Acceptable Use

Users are expected to utilise the network and Wi-Fi systems in a responsible manner. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion. Below is a set of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the school code of conduct.

1	I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the school into disrepute.
2	I will use appropriate language – I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3	I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4	I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.
5	Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person in accordance with the GPDR. I will not reveal any of my personal information to students.
6	I will not trespass into other users' files or folders.

7	I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users.
8	I will ensure that if I think someone has learned my password then I will change it immediately and/or contact the school business manager or those named persons already specified.
9	I will ensure that I log off after my network session has finished.
10	If I find an unattended machine logged on under other users' username, I will **not** continue using the machine – I will log it off immediately.
11	I will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the school leadership team.
12	I am aware that e-mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.
13	I will not use the network in any way that would disrupt use of the network by others.
14	I will report any accidental access, receipt of inappropriate materials or filtering breaches/ unsuitable websites to contact the school business manager or those named persons already specified.
15	I will not use "USB drives", portable hard-drives, "floppy disks" or personal laptops on the network without having them "approved" by the school checked for viruses.
16	I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
17	I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed. Any new software must be installed by an approved school technician
18	I will not accept invitations from children and young people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine. As damage to professional reputations can inadvertently be caused by quite innocent postings or images - I will also be careful with who has access to my pages through friends and friends of friends. Especially with those connected with my professional duties, such a school parents and their children.
19	I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to, are not confused with my professional role in any way.
20	I will support and promote the school's e-safety and Data Security policies and help pupils be safe and responsible in their use of the Internet and related technologies.
21	I will not send or publish material that violates GPDR or breaching the security this requires for personal data.
22	I will not receive, send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting.
23	I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.
24	I will ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used. Breach of this may invalidate school insurance.
25	I will ensure that any Personal Data (GDPR) that is sent over the Internet will be encrypted or otherwise secured.

4. Services

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

5. Network Security

Users are expected to inform the school resource manager, or those named persons already specified, immediately if a security problem is identified and should not demonstrate this problem to other users. Files held on the school's network will be regularly checked by authorised ICT technicians and staff. Users identified as a security risk will be denied access to the network.

6. Media Publications & Permissions

Written permission from parents or carers must be obtained before photographs or videos of pupils are published. Also, examples of pupils' ICT or computing work must only be published (e.g. photographs, videos, TV presentations, web pages etc.) if written parental consent has been given.

END

POSITION	Headteacher	**NAME**		**SIGNATURE**		**DATE**	
POSITION	Governor	**NAME**		**SIGNATURE**		**DATE**	
POSITION		**NAME**		**SIGNATURE**		**DATE**	