Leventhorpe
a business and enterprise academy

Policy Title:	ICT Acceptable Use (Staff)
Policy no:	R 8
Committee:	Resources
Main Staff Link:	JCM
Due for Review:	**Spring 2020**

ICT Acceptable Use Policy – Staff

Leventhorpe makes available to staff various forms of electronic media and services, including computers, e-mail, telephones, voicemail and the internet. All staff and everyone connected with the school should remember that the electronic media and services provided by the school are school property and their purpose is to facilitate and support school business. All users have the responsibility to use these resources in a professional, ethical, and lawful manner.

No policy can lay down rules to cover every possible situation. This policy is designed to set down general principles that all staff are expected to adhere to when using electronic media and services. Staff are expected to use any school equipment responsibly at all times.

Prohibited Communications
School equipment and electronic media should not be used for transmitting, retrieving, or storing any communication or document that is:

1. Discriminatory or harassing
2. Derogatory to any individual or group
3. Obscene or pornographic
4. Defamatory or threatening
5. In violation of any licence governing the use of software
6. Illegal or contrary to any school policy or interests

Mobile Phones - Staff should not ordinarily use their personal mobile telephones to communicate with students except in emergencies, nor should they give their mobile phone number to students. The school has mobile telephones which are available to be used on school trips/visits etc

Personal Details - do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.

Passwords and Personal Data - do not disclose any passwords and ensure that personal data (such as data held on SIMS software) is kept secure and used appropriately.

Duty to Report - staff have a duty to report any eSafety incident or loss of equipment belonging to the school or themselves which may impact on their professionalism or the school.

Access to Employee Communications
Staff should not assume electronic communications are completely private. If they have sensitive information to transmit, they should use other means. Authorised staff may, without prior notice, access the email account of someone who is absent from school (or who has left the school) in order to deal with any school-related issues retained on that email account.

All staff should be aware that the school may gather logs for most electronic activities or monitor staff communications directly, e.g. telephone numbers dialled, sites accessed, call length.

The school reserves the right, at its discretion, to review any member of staff's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other school policies.

Security/Appropriate Use
Staff must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorisation has been granted by school management, staff are prohibited from engaging in, or attempting to engage in:

1. Monitoring or intercepting the files or electronic communications of other employees or third parties
2. Hacking or obtaining access to systems or accounts they are not authorised to use
3. Using other people's log-ins or passwords
4. Breaching, testing, or monitoring computer or network security measures.

No e-mail or other electronic communications should be sent that attempt to hide the identity of the sender or represent the sender as someone else.

Anyone obtaining electronic access to other companies' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner or other licence.

Staff are expected to keep any portable equipment (e.g. laptops) secure. Personal data (e.g. personal student data) should not be stored on portable devices unless those devices are encrypted by the school. The school will provide remote access to school data via a portal which does not have the ability to store data locally

Any school equipment loaned by the school remains the property of the school at all times. When a member of staff ceases to be employed by the school they must return all school property and ensure that they obtain a signed receipt. Failure to do so will result in the school taking steps to recover the property.

Social Media

We publish information about our school and communicate with parents / carers in many ways:

- our own website
- parents' consultations and informal meetings
- newsletters, email and text messages
- social media (e.g. Twitter)

We welcome anyone who is interested in the life of our school to follow us and connect with us through our school website, newsletter and any other media platforms that we use. These sites allow us to communicate more about day-to-day life in school.

Use of sites

It is important for everybody's safety that we are clear about how we use these sites and what constitutes acceptable behaviour from the people who choose to follow us. We use our website and social media sites to publish information that is of general interest. They are not appropriate places to discuss personal matters that are specific to individual members of our community, whether that is students, parents or staff.

Respect

- We will not tolerate any form of bullying on social media and will take appropriate action to remove any offensive communications, posts or comments that refer to specific, individual matters between the school and members of its community
- We will not tolerate any comments or posts that are defamatory, rude or abusive towards any member of our school community, whether that be students, parents, staff or governors, or the school itself

Policy for staff usage

1. Staff members must not have contact through any personal accounts on social media channels with any student, unless the students are family members. This includes following students on Twitter or befriending students on Facebook

2. Staff must be conscious at all times of the need to keep their personal and professional lives separate. Staff should not put themselves in a position where there is a conflict between their work for the school and their personal interests.

3. Staff must not engage in activities involving social media which might bring the school into disrepute.

4. Staff must not represent their personal views as those of the school's on any social medium.

5. Staff must not discuss personal information about students, parents, staff or the school or any other professionals they interact with as part of their job on social media.

6. Staff must not use social media and the internet in any way to attack, insult, abuse or defame students, their family members, colleagues, other professionals, other organisations, or the school.

   Staff must be accurate, fair and transparent when creating or altering online sources of information on behalf of the school.

7. Staff members are strongly advised to ensure that they set the privacy levels of their personal accounts as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers or other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

8. If staff need to communicate with students through social media or to enable students to keep in touch with one another, they can only do so with the approval of the school and through official school accounts. In the first instance, staff are advised to use the forum and chat facilities within the school's VLE.

9. When using official school accounts on social media every effort should be made to maintain students' privacy.

10. Official School accounts should be open/public access so that all communication is transparent and not make use of private messaging tools. (Private messages should be sent via email on school accounts

11. Staff should not discuss the performance of students via Social Media.

Violations

Any member of staff who abuses the privilege of their access to e-mail or the Internet in violation of this policy will be subject to disciplinary action, including possible termination of employment, legal action, and criminal liability.

Staff Protection

The school has a duty of care to all staff and will not tolerate abuse or harassment connected with issues within school or against any member of staff. Should any member of staff feel that they have been harassed or abused on a social media site connected with the school or otherwise in connection with their employment at the school they should report it to the Personnel Manager so that appropriate action can be taken.