ACCEPTABLE USE POLICY - STAFF

A STAFF GUIDE FOR ACCEPTABLE USE OF IT INSIDE AND OUTSIDE FULFORD SCHOOL

UPDATED SEPTEMBER 2019

Fulford School

Realising Potential | Creating the Future

CONTENTS

1.0 PRINCIPLE & INTRODUCTION

1.1 Introduction

In May 2018 the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) became enforceable across the United Kingdom. As part of School Name's programme to comply with the new legislation it has written a new suite of Information Governance policies.

The Acceptable Use policy governs the use of the School's corporate network that individuals use on a daily basis in order to carry out business functions.

This policy should be read in conjunction with the other policies in the School's Information Governance policy framework.

1.2 The school has provided computers for use by staff as an important tool for teaching, learning, and administration of the school. Use of school computers, by both members of staff and pupils, is governed at all times by the following policy. Please ensure you understand your responsibilities under this policy, and direct any questions or concerns to the IT Department in the first instance.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. Deliberate abuse of the school's computer system may result in disciplinary action (including possible termination), and civil and/or criminal liability.

Please note that use of the school network is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the school and staff, to safeguard the reputation of the school, and to ensure the safety of all users. Please respect these guidelines, many of which are in place for your protection.

Lastly, the school recognises that the distinction between computer use at work and at home is increasingly blurred, with many of us now using our own computers for work. While the school neither wishes nor intends to dictate how you use your own computer, staff should consider that the spirit of this policy applies whenever you are undertaking an activity that stems from your employment with the school.

1.3 Scope

All policies in Fulford School Information Governance policy framework apply to all School employees, any authorised agents working on behalf of the School, including temporary or agency employees, and third party contractors. Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

- The policies apply to information in all forms including, but not limited to:
- Hard copy or documents printed or written on paper,
- Information or data stored electronically, including scanned images,
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer,
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card,
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops,
- Speech, voice recordings and verbal communications, including voicemail,
- Published web content, for example intranet and internet,

Photographs and other digital images.

2.0 COMPUTER SECURITY AND DATA PROTECTION

2.1 You will be provided with a personal account for accessing the computer system, with your own username and password. This account will be tailored to the level of access you require, and it is for your use only. As such, you must not disclose your password to anyone, including IT support staff. If you do so, you will be required to change your password immediately.

2.2 It is accepted that students may be allowed to use staff accounts for administrative tasks, such as entering House Points onto SIMS. This access must be strictly monitored by you and must only be for administrative work. This access is granted entirely at your own risk. It is recommended that work of this nature be displayed on the projector so it can be closely monitored. Any security breech as a result of granting this access could result in disciplinary action.

2.3 When leaving a computer unattended, you must ensure you have either logged off your account, or locked the computer to prevent anyone using your account in your absence.

2.4 You must not store any sensitive or personal information about staff or students on any portable storage system (such as a USB memory stick or portable hard disk) **unless that storage system is encrypted and approved for such use by the school.**

2.4.1 **In rare circumstances a need may arise that requires a member of staff to transport confidential data. In these circumstances, staff authorised by the Head teacher to transport this data must use encrypted memory sticks. Failure to do so could result in disciplinary action. Use of encrypted memory sticks must be directly authorised by the Headteacher.**

2.5 When publishing or transmitting non-sensitive material outside of the school, you must take steps to protect the identity of any pupils.

2.6 If you use a personal computer, laptop or tablet at home for work related purposes, you must not store any school-related sensitive or personal information on the computer unless the whole device is encrypted.

2.6.1 If you are required to hold this information for work related purposes, you must seek the written permission of the Headteacher and ensure than your personal computer is secured to stop non-staff members accessing the data.

2.7 It is recommend that you make backups of data kept on any storage system other than the network storage drives or your 'Documents' folder. This includes USB memory sticks or a personal computer.

2.8 You must ensure that items of portable computer equipment (such as laptops, digital cameras, or portable projectors) are securely stored in a locked room or cupboard when left unattended.

2.9 IT equipment is **not** allowed to be taken offsite without the explicit permission of the Technical Services Manager / System Administrator.

3.0 PERSONAL USE

3.1 The school recognises that occasional personal use of the school's computers is beneficial both to the development of your IT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use:

3.1.1 must comply with all other conditions of this ACCEPTABLE USE POLICY as they apply to non-personal use, and all other school policies regarding staff conduct;

3.1.2 must not interfere in any way with your other duties or those of any other member of staff;

3.1.3 must not have any undue effect on the performance of the computer system; and 3.1.4 must not

be for any commercial purpose or gain unless explicitly authorised by the school.

3.2 Personal use is permitted at the discretion of the school and can be limited or revoked at any time.

3.3 IT support staff monitor all network usage regardless of whether it is work related or otherwise. If you access personal information that you wish to remain confidential you do so at your own risk.

3.5 Staff are **not** permitted to store non-school related materials on network drives or their 'Documents' area such as

- Music
- Games
- Videos
- Images / Photographs

If such material is found, it will be removed without notice.

4.0 USE OF YOUR OWN EQUIPMENT – BRING YOUR OWN DEVICE

4.1 You must not connect personal computer equipment to school computer equipment without prior approval from IT Support staff, with the exception of storage devices such as USB memory sticks.

4.2 If you keep files on a personal storage device (such as a USB memory stick), you must ensure that other computers you connect this storage device to (such as your own computers at home) have an up-to-date anti-virus system running to protect against the proliferation of harmful software onto the school computer system.

4.3 You must never directly connect (hardwire) your own device onto the school network.

4.4 The wireless network is provided for your own convenience and the school does not guarantee its availability or compatibility with your own device but has endeavoured to make as many devices compatible with it as possible. If your device is not compatible with the wireless network the IT support staff will be unable to assist you.

4.5 Devices brought into school are done so at your own risk. Any damage or loss to your device while on school property will not be covered by the school. When not in use, you are advised to leave your device in a secure location.

4.6 School related videos and photos of a sensitive or personal nature (i.e. containing images of people) should not be held on any personal device e.g. Mobile Phones/Tablets (see Code of Conduct)

5.0 CONDUCT

5.1 You must at all times conduct your computer usage professionally, which includes being polite and using the system in a safe, legal, manner that does not tarnish the reputation of the School. Among uses that are considered unacceptable are the following:

5.1.1 Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;

5.1.2 Making ethnic, sexual-preference, or gender-related slurs or jokes.

5.2 You must respect, and not attempt to bypass, security or access restrictions in place on the computer system.

5.3 You must not intentionally damage, disable, or otherwise harm the operation of computers.

5.4 You must make efforts not to intentionally waste resources. Examples of resource wastage include:

5.4.1 Excessive downloading of material from the Internet;

5.4.2 Excessive storage of unnecessary files on the network storage areas;

5.4.3 Use of computer printers to produce class sets of materials, instead of using photocopiers.

5.5 You should avoid eating or drinking around computer equipment.

5.6 Other Business Use

5.6.1 Users are not permitted to use computer equipment to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of School management.

5.6.2 Employees understand that School management may have access to their internet browsers and browsing history contained within,

5.6.3 Employees understand that the School reserves the right to suspend internet access at any time,

5.6.4 Use of the internet for personal use does not infringe on business functions

5.7 All use of the Internet is governed by City of York Council and is subject to their Acceptable Use Policy as well as the guidelines listed here. A copy of their Electronic Communications Policy can be found here.

6.0 USE OF SOCIAL NETWORKING WEBSITES AND ONLINE FORUMS

6.1 Staff must take care when using social networking websites such as Facebook or Twitter, even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.

6.2 You must not allow any pupil to access personal information you post on a social networking site. In particular:

6.2.1 You must not add a pupil to your 'friends list'.

6.2.2 You must ensure that personal information is not accessible via a 'Public' setting, but ensure it is set to a 'Friends only' level of visibility.

6.2.3 You should avoid contacting any pupil privately via a social networking website, even for school-related purposes.

6.2.4 You should take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them access to your personal information.

6.3 Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

6.3.1 Unless authorised to do so, you must not post content on websites that may appear as if you are speaking for the school.

6.3.2 You should not post any material online that can be clearly linked to the school that may damage the school's reputation.

6.3.3 You should avoid posting any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass, or defame the subject.

6.4 Staff and students are prohibited from accessing Facebook from within school, with the exception of some authorised staff for child protection purposes.

6.5 Staff must not contact students from their personal email addresses and must use the school email system at all times.

6.6 These guidelines are in addition to the guidelines stated in the **Staff Handbook** under the heading **"Staff Code of Conduct", "Keeping Children Safe in Education"** and **"What to do if you're worried a child is being abused"**.

7.0 USE OF EMAIL, TELEPHONe, MOBILE DEVICES AND REMOTE WORKING

7.1 All members of staff with a computer account are provided with an email address for communication both internally and with other email users outside the school. The following considerations must be made when communicating by email:

7.1.1 E-mail has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of e-mails may therefore have to be made available to third parties. You must be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for e-mail.

7.1.2 E-mail to outside organisations has the same power to create a binding contract as hardcopy documents. Check e-mail as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal advice before sending. You must not purchase goods or services on behalf of the school via e-mail without proper authorisation.

7.1.3 E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, you must not send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential information belonging to the school.

7.1.4 Having an external e-mail address may lead to receipt of unsolicited e-mail containing offensive and/or sexually explicit content. The school will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users from the Internet.

7.1.5 You must not send chain letters or unsolicited commercial e-mail (also known as SPAM).

7.2 Email Security

7.2.1 Users will take care to use their email accounts in accordance with the School's information security policy. In particular users will:

7.2.2 Not click on links in emails from un-trusted or unverified sources,

7.2.3 Use secure email transmission methods when sending personal data,

7.2.4 Not sign up to marketing material that could jeopardise the School's IT network,

7.2.5 Not send excessively large email attachments without authorisation from School management and the School's IT provider.

7.2.6 Group Email Accounts. Individuals may also be permitted access to send and receive emails from group and/or generic email accounts. These group email accounts must not be used in a personal capacity.

7.3 While it is possible to link tablet devices or smartphones to the school email system, **staff must first seek written permission of the Head teacher in order to do so, and then inform the IT Networks Department**. IT Support Staff will then assist you with your device, and check your phone to ensure that there is a passcode, PIN, or pattern unlock required to gain access to the device.

7.3.1 **In the event that your device is lost or stolen, you must inform the school immediately**, the police if appropriate and contact your service provider to attempt to disable the device. At the schools discretion, we may attempt to remote wipe your device in order to maintain the security of our network and its data.

7.4 The school provides remote access to our system via a Securel VPN connection. The school also provides access to email via Outlook Web App.

Both of these methods are encrypted and secure connections. Where possible staff should use these methods when accessing confidential data, such as student records.

7.4.1 In order to use our remote services, your home PC must have up to date endpoint security software installed and working.

7.5 These guidelines are in addition to the guidelines stated in the **Staff Handbook “Staff Code of Conduct”, “Keeping Children Safe in Education”** and **“What to do if you’re worried a child is being abused”**.

7.6 Telephone and Skype Use

7.6.1 The School provides access to telephones and skype accounts to employees to assist with performance of their duties. These should be used in with regard to the other sections (4 and 5 in particular) and The School also allows employees to use Skype for Business. For the benefit of doubt Skype calls are classed as telephone calls in this policy.

.

8.0 SUPERVISION OF PUPIL USE

8.1 Pupils must be supervised at all times when using school computer equipment or mobile devices in lesson and when arranging use of computer facilities for pupils, you must ensure supervision is available.

There must be a sound educational purpose behind a decision to allow students to use mobile devices during a lesson. When these occasions arise, staff should indicate that the use of mobile devices is appropriate by displaying the relevant ‘Mobile Devices Allowed’ notice that is displayed in every classroom. At other times, the default notice ‘Mobile Devices Not Allowed’ should be displayed. Staff are responsible for ensuring that the students use mobile devices appropriately.

8.2 Supervising staff are responsible for ensuring that the separate Acceptable Use Policy for pupils is enforced.

8.3 Supervising staff must ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of computer use by pupils. Please click here to view a copy of the schools e-safety policy.

8.4 If you suspect a student of violating the Acceptable Use Policy, you must contact the IT Support Helpdesk who will then contact Student Support if a violation has been committed.

8.5 Staff should be aware that students are also banned from using social media sites on mobile devices. Some students may be able to access such sites through their mobile devices via mobile broadband connections. Please see section 12.0 of this document if you suspect a student of visiting a banned website.

9.0 PRIVACY

9.1 Use of the school computer system, including your email account and storage areas provided for your use, may be subject to monitoring by the school to ensure compliance with this Acceptable Use Policy and applicable laws. This may include remote monitoring of an interactive logon session. In particular, the school does keep a complete record of sites visited on the Internet by both pupils and staff, however, usernames and passwords used on those sites are NOT monitored or recorded.

9.2 You should avoid storing sensitive personal information on the school computer system that is unrelated to school activities (such as personal passwords, photographs, or financial information).

9.3 The school may also use measures to audit use of computer systems for performance and diagnostic purposes.

9.4 Use of the school computer system indicates your consent to the above described monitoring taking place.

10.0 CONFIDENTIALITY AND COPYRIGHT

10.1 Respect the work and ownership rights of people outside the school, as well as other staff or pupils.

10.2 You are responsible for complying with copyright law and licenses that may apply to software, files, graphics, documents, messages, and other material you wish to use, download or copy. Even if materials on the school computer system or the Internet are not marked with the copyright symbol (©), you should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.

10.3 You must consult a member of IT Network staff before placing any order of computer hardware or software, or obtaining and using any software you believe to be free. This is to check that the intended use by the school is permitted under copyright law (as well as to check compatibility and discuss any other implications that the purchase may have). Do not rely on the claims of suppliers, who do not have specific knowledge of the school's systems.

10.4 As per the standard staff contract, any invention, improvement, design, process, information, copyright work, trade mark or trade name made, created or discovered by you during the course of your employment in any way affecting or relating to the business of the School or capable of being used or adapted for use within the School shall be immediately disclosed to the School and shall to the extent permitted by law belong to and be the absolute property of the School.

10.5 By storing or creating any personal documents or files on the school computer system, you grant the school a nonexclusive, universal, perpetual, irrevocable, and royalty-free license to use, copy, and distribute those documents or files in any way the school sees fit.

11.0 REPORTING PROBLEMS WITH THE COMPUTER SYSTEM

11.1 It is the job of the IT Network Department to ensure that the school computer system is working optimally at all times and that any faults are rectified as soon as possible. To this end:

11.1.1 You should report any problems that need attention to a member of IT support staff as soon as is feasible. Problems that seriously hinder your job or teaching and require immediate attention should be reported by telephone; any other problem must be reported via the online Support Request system.

11.1.2 If you suspect your computer has been affected by a virus or other malware, you must report this to a member of IT Network staff immediately.

11.1.3 If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, the lesser the chances of your data being recoverable (mere minutes can count).

12.0 REPORTING BREACHES OF THIS POLICY

12.1 All members of staff have a duty to ensure this Acceptable Use Policy is followed. You must immediately inform a member of the IT support staff, or the Head teacher, of abuse of any part of the computer system. In particular, you should report:

12.1.1 any websites accessible from within school that you feel are unsuitable for staff or student consumption;

12.1.2 any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc;

12.1.3 any breaches, or attempted breaches, of computer security; or

12.1.4 any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the school computer system.

12.2 Reports should be made either via email or the online Support Request system. All reports will be treated confidentially.

13.0 REVIEW AND EVALUATION

13.1 This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.

14.0 DECLARATION

STAFF MEMBER

Please complete and return this page to the School Office.

As a user of the Fulford School Network and associated services, I agree to comply with the rules, as explained within the Acceptable Use Policy.

Name: …………………………………………………………………………………………….

Signature: …………………………………………………………………………………………….

Date: …………………………………………………………………………………………….

NOTES

a. "Sensitive personal information" is defined as information about an individual that is protected by law under the Data Protection Act 1998. Examples of such data include addresses and contact details of individuals, dates of birth, and pupil SEN data. This list is not exhaustive. Further information can be found in the school’s Data Protection Policy.