ICT Acceptable Use Policy

Contents Page

Appendices

POLICY STATEMENT

The Constellation Trust is a forward thinking and innovative organisation where a passionate and dynamic team work together to maximise opportunities in the best interest of our pupils. Together we make a difference.

Our Trust prides itself on providing a friendly, caring, family of schools where everything we do is for the benefit of the children and families that we serve. We encourage pupils to have a 'love of learning' so that they become life-long learners and achieve to the very best of their abilities.

The purpose of this policy is to ensure that employees, workers and other people accessing Trust Information Communication Technology (ICT) understand the ways in which the ICT equipment and Wi-Fi is to be used. Our aim is to provide a service within schools to promote educational excellence in ICT, innovation, communication and educating users about online behaviour, including interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness. The policy aims to ensure that ICT facilities and the Internet are used effectively for their intended purpose, without infringing legal requirements or creating unnecessary risk. Where reference is made to Trust ICT, this also includes any school specific facilities, equipment and networks. Any reference to Trust includes all its schools.

The policy and guidelines cover use of the internet both within and beyond the Trust when the internet is accessed using Trust equipment, e.g. using a Trust laptop or by remotely accessing the Trust network; however, it is not essential for staff to work at home.

Employees are provided with free access to a wide range of ICT provision to enable and assist their work and support their educational development. By using the Trust's provision and the Trust's devices, or using personal devices on-site, which may require access to the Trust's Guest Wi-Fi, all users are agreeing to adhere to this policy. When logging on to any computer in the Trust, users are presented regularly with an informational message that alerts them to the fact that they are bound by the terms in this, and all related policies. This is also a required read via the HR Every portal.

Users are responsible and personally accountable for their use and activity on the Trust's ICT systems and Wi-Fi. Any use that contravenes this policy may result in the Trust Disciplinary Policy and Procedure being invoked. In addition, ICT usage privileges may be withdrawn or reduced.

Summary of Policy - Main Points

Below is a short summary of the policy's main points. However, they should be read in conjunction with the rest of the policy in its entirety.

a) This policy applies to ALL employees, workers and others accessing ICT at The Constellation Trust.
b) Any breaches of this policy must be reported to RM / the Headteacher or the Head of Digital Solutions immediately.
c) **Passwords** – must be kept safe and must remain confidential at ALL times.
d) **Software** - no software must be installed unless by RM – requests must go through the Trust.
e) **Viruses** - No viruses must be introduced.
f) **USB access** is blocked – please see exceptions in section 4.2.
g) **E-communications** must be appropriate – please see section 4.3. If any inappropriate material is accessed accidentally, then line managers / RM must be informed immediately.
h) **Trust devices** - Staff should be using Trust devices at all times as they are monitored and regulated – users are personally accountable for their use of Trust ICT systems and networks.
i) **Guest Wi-Fi** will only be given by RM with Trust approval.
j) **Copyright** must not be breached whilst using Trust's ICT systems.
k) **Multi Factor Authentication** – all users must use MFA when remotely accessing the network via RM Unify.
l) **Social media** – users must not reflect the Trust in any inappropriate way. The Trust no longer uses Twitter/X as a social media platform. Staff are advised not to communicate to students via social network sites. Staff should ensure their privacy policies are set correctly on their personal social media accounts.
m) Users must not **misuse** the Trust's ICT networks – please see section 4.13.
n) **Internet** – users must not circumvent the Trust's firewall and internet filtering systems by using proxy servers and websites. DSL's take lead responsibility for safeguarding and online safety. Students should never access the internet via a staff login. Staff must not misuse the internet facilities – please see section 7 for more details.
o) **Emails** – they are monitored and can be used as evidential records. All electronic communication between staff and students must use the Trust's ICT systems. 2-factor MFA is enforced when accessing the Trust's email facilities outside Trust buildings. If a suspicious email is received, staff should seek advice from RM for advice.

By clicking 'Acknowledge' in your Every account, you agree to the rules detailed in this Acceptable Use Policy and the potential consequences of non-compliance.

1 SCOPE

1.1 This policy applies to all employees, workers and others accessing ICT at The Constellation Trust and they will be termed as 'users' within this policy. This policy details the Trust's expectations of all users of the Trust's electronic communication, including, but not limited to telephone, social media platforms, email, internet and ICT systems.

2 ROLES AND RESPONSIBILITIES

2.1 The Trust Board is responsible for approving this policy. The CEO is responsible for ensuring that staff and managers are aware of and adhere to this policy and procedures and that breaches are managed swiftly, effectively, fairly and consistently. The managed service provider RM will limit access to websites and may be directed to monitor usage and report any breaches to the Head of Digital Solutions, the Headteacher or the CEO. Managers must ensure they report any breaches of this policy immediately to RM or the Head of Digital Solutions. Data protection breaches must also be reported to the Data Protection Officer.

2.2 All users must ensure they understand and adhere to the Trust's expectations regarding electronic usage and communications, seeking further clarification and advice where appropriate. If they require access to a website, which is blocked, they should raise the issue with their line manager and then the DSL in each school who will forward a request to RM. The Trust will also be kept informed.

3 EQUALITY AND DIVERSITY

3.1 The Constellation Trust is committed to:

- Promoting equality and diversity in its policies, procedures and guidelines
- Ensuring staff are protected from unlawful direct or indirect discrimination resulting from a protected characteristic (e.g. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex or sexual orientation)

4 KEY PRINCIPLES

a. Summary - This policy details the minimum expectations of the Trust when users are accessing Trust ICT systems and Wi-Fi. Failure to comply with these requirements may be viewed as a breach of this policy and could be viewed as a disciplinary matter, with serious breaches potentially leading to dismissal.

4.2 General

- Passwords and login details must remain confidential at all times

• Users must not intentionally install software - RM must install all software

• Users must not intentionally introduce viruses or other malicious software - **NO** external hard drives or memory sticks are permitted. The only exception to this is where SD card readers are permitted for downloading photographs / video files from secondary school SLR cameras – this is limited to certain desktops within schools (high spec media suites at North and West). Other specific devices eg; Trust iPads, student exam laptops and certain digital cameras are unblocked and may be connected via USB cables – these requests must come through Trust approval and once allowed, RM will facilitate unblocking the device.

4.3 E-communications systems

• The Trust's e-communications systems must not be used to store, send or distribute messages or material which may be perceived by the recipient or the Trust as:

- Aggressive, threatening, abusive or obscene
- Sexually suggestive
- Defamatory
- Sexually explicit
- Discriminatory comments, remarks or jokes
- Offensive
- Act in a way that contravenes the Trust's Expectations and Code of Conduct, other Trust or school policies, legislative, statutory or professional requirements
- Bring the Trust into disrepute
- Disclose sensitive information or personal data to unapproved people or organisations
- Breach the Trust's Data Protection Policy, General Data Protection Regulations or the Data Protection Act 2018
- Intentionally access or download material containing sexual, discriminatory, offensive or illegal material
- Participate in online gambling, including lotteries
- Participate in online auctions unless authorised to do so for work-related matters
- Originate or participate in email chain letters or similar types of communication
- Harass or bully another person
- Create material with the intent to defraud

4.4 Inappropriate material

If a user accidentally accesses inappropriate material on the internet or by email, they must immediately disconnect and inform their line manager and / or RM.

Users must not bring into school **any** material that would be considered inappropriate. This includes files stored on memory sticks, CD, DVD or any other electronic storage medium, or accessing information via the Trust's Wi-Fi, which would be viewed inappropriate.

Under no circumstances should any users of the Trust or school's ICT systems download, upload or bring into school material that is unsuitable for children or schools. This includes any material of a violent, racist or inappropriate sexual nature. The transmission, display, storage or promotion of any such material is a violation of the Computer Misuse Act 1990, and possession of certain types of material can lead to police prosecution. If in any doubt, staff should check with their line manager and / or RM. Staff are also encouraged to refer to the film classification system as a guide.

Users must not use the Trust ICT systems or Wi-Fi for the creation, transmission or access of pornographic, illegal or gambling content.

4.5 Personal use of ICT equipment and guest Wi-Fi

Occasional appropriate and reasonable personal use of ICT equipment and/or guest Wi-Fi on-site is permitted provided such use of the Trust systems:

- Is restricted to the user's own time
- Doesn't interfere with the performance of duties
- Doesn't adversely impact on the performance of the Trust's ICT systems or the network
- Doesn't contravene the requirements of the Trust's Code of Conduct, or other Trust or school policies
- Doesn't include material of a pornographic, illegal, or gambling nature

Staff should be using Trust devices at all times as they are monitored and therefore regulated. Personal laptops / devices are not permitted to join the main networks – these are unregulated devices and pose serious security threats to the entire Trust network. Guest Wi-Fi will only be given by RM with Trust approval. This will then limit certain permissions. Certain external users such as NHS staff, Hull City Council Music Service providers and iPass staff need to approach RM to allow the relevant VPN access to be allowed. These secure encrypted channels allow external visitors to access both their own systems and our network.

4.6 Personal accountability

Users must always be mindful that they are responsible and personally accountable for their use of Trust ICT systems and networks. All internet-based activity on personal devices is monitored and logged whilst using the guest Wi-Fi. Misuse of Trust ICT systems and networks belonging to, or associated with the Trust may breach the Code of Conduct, other

policies and/or procedures and/or the law. Users can be held personally liable and such breaches may lead to civil, criminal or disciplinary action including dismissal.

Users are responsible for all files that are stored in their storage area and any visits to websites by their user account.

4.7 Copyright

Users must not breach the copyright of any materials whilst using the Trust's ICT systems. This includes, but is not exclusive to:

• Copying, or attempting to copy, any of the school's software

• Storing any files in their personal storage area which require copyright permission, and where that permission is not held.

Any breach of copyright whilst using the Trust's ICT systems is the individual user's responsibility and the Trust cannot accept any liability or litigation for such a breach.

4.8 Confidentiality and data security

Users must ensure that:

• They keep personal data safe, taking steps to minimise the risk of loss or misuse of data

• Personally identifiable and sensitive, confidential data is protected with the use of passwords, locking of computers, logging off shared devices, use of encryptions where appropriate and remote access rather than transporting or transferring information. This is facilitated through RM Unify. (Please see section 7 of this policy)

• Personally identifiable, sensitive and confidential data must not be stored on any form of removable media (e.g. memory sticks, external hard-drives, surfaces or laptops, and CDs or DVDs) and it must not be stored on users' personal devices (e.g. home PCs, mobile phones)

• When using mobile devices, users encrypt/password protect documents; password protect the device; ensure the device has appropriate virus and malware checking software

• Data is only retained, destroyed and deleted safely in line with the Trust's Data Protection Policy and associated procedures and guidelines

4.9 Multi Factor Authentication

All Trust laptops are managed by RM via Microsoft Intune. When remotely accessing the network through RM Unify, users must use Multi-Factor Authentication.

Users must not save sensitive data on any form of unencrypted portable device.

4.10 Software requests

Users must not download, copy or attempt to install any software onto Trust computers/devices. Any software requests need to be made through the Head of Digital Solutions using the correct procedures found in the Trust area of SharePoint. There are often costs involved when adding software such as ongoing subscription costs, the initial software costs and the costs associated with packaging and testing the software by RM.

4.11 Hacking

Any attempt by a user to compromise the security or functionality of the Trust networks and its ICT systems, either internally or externally, will be considered as “hacking”. It should be noted that “hacking” is illegal under the Computer Misuse Act 1990 and is prosecutable under law. Users must not deliberately attempt to gain unauthorised access to networked facilities or services, including any attempt to probe, scan or test the vulnerability of the system or network. All Trust machines connected to the Trust's ICT networks have appropriate, fully functioning and up to date anti-virus software and malware protection.

4.12 Social media

Users must not discuss or post content that reflects the Trust or its employees in an inappropriate or defamatory manner through any electronic communication methods. This includes posting to social networking sites.

As a Trust, we do not allow the use of Twitter/X as a social media platform.

4.13 Misuse

Users must not carry out any of the following deliberate activities:

• corrupting or destroying other users' data

• violating the privacy of other users

• disrupting the work of others

• denying service to other users (for example, by deliberate or reckless overloading of the network)

• continuing to use an item of networking software or hardware after the Trust has requested that use cease because it is causing disruption to the correct functioning of the school's ICT systems and/or networks

• other misuse of the Trust's ICT and networked resources, such as the introduction of viruses or other harmful software to the Trust's ICT systems

• unauthorised monitoring of data or traffic on the Trust's ICT network or systems without the express authorisation of the owner of the network or systems

This policy still applies when users access any of the Trust's systems off-site.

4.14 Internet

The Trust wishes to encourage all users to use the internet, however it is provided for work purposes and any use of the internet for personal reasons must be carried out in the user's free time. The Trust cannot be held responsible for any failed personal financial transaction that may happen whilst using the Trust's ICT systems.

Any attempt to circumvent the Trust's firewall and internet filtering systems will be treated as a breach of this policy. This includes the use of proxy servers and websites to bypass the internet filtering systems. Such activity will be subject to the Trust's Disciplinary Procedure in addition to any disciplinary outcome or sanction; it could also result in the removal of access to the Trust's ICT systems or internet access.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both the safeguarding and RM teams to be effective. The DSL's should work closely together with RM to meet the needs of our schools.

There is a wealth of information on the internet; however, due to the open nature of the internet, some material is either illegal or unacceptable. Any user who thinks inappropriate or illegal material is being accessed must report it to their line manager and the DSL's.

The DSL takes lead responsibility for safeguarding and online safety, which includes overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

RM have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

Whether users are using on-site Trust equipment, Trust equipment off-site or their own device via the Trust network (eg; personal mobile phone), users should:

• limit personal use of the internet to own time

• take advice from line managers before downloading large files or sending large amounts of data via a web-link – to avoid adversely impacting on the performance of the systems these transactions can be scheduled for off-peak times. Please contact the Head of Digital Solutions if you require a large data transfer to an external user (outside of the Trust).

• if users accidentally access inappropriate material including unexpected 'pop-ups' they must disconnect immediately and inform their line manager and/or RM.

Users must be mindful that if they use Trust equipment off-site, they need to minimise the risk of inappropriate information presenting on their Trust equipment whilst at work. For example, the acceptance of cookies can result in pop-ups, which may contain material, which is inappropriate for school environments. Users who have been issued a Trust mobile phone should not:

• access or download material which is pornographic, illegal or of a gambling nature

• use the internet for personal use during working time, even if minimised on the screen

• use systems to participate in on-line gambling or on-line auctions

• download music or video files unless for Trust or school purposes

• use 'peer to peer' or other file sharing services except where authorised to do so

5 MOBILE PHONES

5.1 Staff should keep personal phone numbers private and not use their own mobile phones to contact pupils or parents. Staff should, wherever possible, not use their own personal mobile phones to take photographs of students. If photographs are taken, they should be permanently deleted immediately from the device.

5.2 Trips and Visits

Staff should only use a Trust mobile phone when on a Trust trip. Staff should not use their own personal mobile phones to take photographs of students on school visits. Staff should not use mobile phones in classrooms in front of pupils, unless they have sought permission from their line manager to do so as part of their lesson.

5.3 Mobile phone security - staff should keep mobile phones secure whilst on Trust premises and report thefts to the police and mobile operator as soon as possible.

6 EMAIL AND ELECTRONIC COMMUNICATION

6.1 When using Trust equipment, networks, email and electronic communication, the Trust expects all users to act responsibly and strictly according to the following conditions:

• Email facilities are provided as a method of enhancing communication of work and school related issues. All users are responsible for the content of the messages that they send.

• Users are reminded that electronic communication can be monitored and random checks may be made.

• Email is the equivalent of a written document and can be used as an evidential record. With this in mind, care and consideration should always be taken before sending an email (e.g. freedom of information requests and subject access requests).

• Where there is a concern that a user has misused the email system, action may be taken in line with the Trust's Disciplinary Procedure.

• All electronic communication between staff and pupils must be carried out through the Trust's ICT systems.

• The Trust has enforced 2-factor authentication when accessing email outside of Trust buildings for staff. Staff are advised not to communicate with pupils via social network sites, texts or telephone calls, although there may be occasions where it is appropriate and necessary (e.g. where staff and pupils are members of external groups or family and friend networks). If staff are unsure, they should seek advice from their line manager in the first instance. Staff must not share personal contact details with pupils (mobile telephone numbers, non-work email addresses, social networking sites etc.) unless there is a justifiable reason (e.g. family or friend networks or external groups) and any unintended breach must be reported to RM and the user's line manager immediately.

6.2 Users who receive emails regarding viruses or security threats must delete the email and report to RM immediately. Users can minimise the risk of inadvertently introducing viruses by permanently deleting without opening emails that look suspicious. Staff are encouraged to contact RM for advice and concerns that a virus may have entered a Trust system should be reported immediately. Users are advised that strict mail filters are in place to prevent any unwanted threat - whilst these measures are never 100% accurate, if you believe a genuine email or link within an email has been blocked, please contact RM for advice. Users should ensure:

• personal email and texts should only take place in their own time, on their own devices

• ensure that their messages are relevant and appropriate to targeted recipients (e.g. not using 'blanket' or 'all-user' emails)

• try to answer emails quickly, politely and professionally

• beware of 'email rage'. Email is quick and easy to use and can encourage ill-considered and even offensive messages

• include a subject heading in every email so that the person receiving it knows what it is about

• inform management/RM immediately if the user receives or sees any offensive or sexually explicit material, spam or phishing communications on the intranet or in email messages at work

• they do not allow email and electronic communication to replace face to face communication

6.3 Access should only be made via the authorised account and password, which must not be made available to any other person.

6.4 Users must not:

• use a password in a way that can be seen by pupils

• use email to circulate material which is illegal, pornographic or of a gambling nature

• use email as a substitute for good verbal communication

• expect to receive a response to emails outside of normal working hours (6pm-6am). If staff are in doubt, they should seek advice from their line manager or RM.

7 THE INTERNET

7.1 The Internet is a series of communication links, which enables computers around the world to access information and exchange files. The Internet allows users to obtain information held (and published) on computers anywhere in the world easily and relatively quickly. It also allows users to send information (such as orders) back to these computers. It is a huge freestanding network to which millions of users have access.

7.2 The legitimate business use of the Internet has increased beyond expectations in the last few years and there are no indications that this increase will not continue. Many organisations now make essential information available only via the Internet.

7.3 The open design of the Internet is its strength. However, the lack of controls and standards also exposes organisations (and private individuals) to an increased risk that networks and systems will be accessed improperly, data corrupted and viruses introduced.

7.4 The Trust believes that the internet is an important and valuable tool and that the ability to use it is a key skill for the 21st century. The Trust is a learning community and it is therefore the Board's viewpoint to support all staff in developing the confidence and ability to access the internet, whilst ensuring that provisions are in place to prevent abuse.

Authorised internet users

7.5 All individual employees will be authorised to use the Trust's Internet facilities by agreeing to this ICT Acceptable Use Policy. All authorised Internet users must be given a

copy of this policy via the HR Every system and confirm they have read and understand the policy and guidelines.

7.6 Under no circumstances should students access the internet using a staff log-in. The Trust has the facility to limit each staff user to only having one log-in if necessary. Staff accounts are set to much higher levels of permissions such as access to YouTube.

7.7 Access should only be made via the authorised account and password, which must not be made available to any other person.

Misuse of the Academy's internet facilities

7.8 Certain types of use of the Internet are unacceptable and they may also be illegal.

7.9 Cases where employees are suspected of intentionally misusing the Academy's Internet facilities, will be investigated and dealt with under the Academy's Disciplinary Procedure.

7.10 Examples of what is considered to be misuse of the Academy's Internet Facilities are given below, but this is not an exhaustive list.

7.11 Use of AI chatbots are not currently permitted on any Trust device and accessing this can be tracked.

7.12 Staff must ensure, whenever practically possible, that the internet is not used by anyone who has not been given authorisation. The lock screen is enabled after a short period of inactivity – staff need to lock their screens after they have enabled presenter mode to prevent GDPR issues or misuse of the internet or access to confidential staff files.

7.13 Access should only be made via the authorised account and password, which must not be made available to any other person.

7.14 In all cases, Internet access must be arranged by the ICT Technical staff and appropriate virus control software must be in place. Such virus protection software must not be "turned off" by non-ICT staff as removing or disabling virus protection software could lead to disciplinary action being taken.

7.15 The Trust reserves the right to disable a user's account if appropriate. The Academy reserves the right to examine or delete any files that may be held on its devices or computers systems. All Internet usage is monitored.

Illegal material

7.16 The vast majority of information on the Internet is of a very interesting and informative nature. Unfortunately, the Internet has also attracted the attention of many of the less desirable elements of modern society and information is available on the Internet which is of an illegal, harmful, pornographic and obscene nature.

Unacceptable Material

7.17 It is illegal to create, access, copy, store, transmit or publish any material, which falls into the following categories:

National Security - Instructions on bomb making, illegal drug production, and terrorist activities;
Protection of Minors - Abusive forms of marketing, violence, and pornography;
Protection of Human Dignity - Incitement to racial hatred or racial discrimination. harassment;
Economic Security - Fraud, instructions on pirating credit cards;
Information Security - Malicious hacking;
Protection of Privacy - Unauthorised communication of personal data, electronic harassment;
Protection of Reputation - Libel, unlawful comparative advertising;
Intellectual Property - Unauthorised distribution of copyrighted works e.g. software or music.

Unacceptable Activity

7.18 It is unacceptable to create, access, copy, store, transmit or publish any material which is:

- Obscene or vulgar.
- Likely to irritate or waste time of others.
- Subversive to the purposes of the Trust.
- Damaged to the reputation of the Trust.

7.19 For the purposes of these guidelines, obscene and vulgar are defined as follows:

- Obscene - Indecent, lewd, repulsive.
- Vulgar - Offending, against good taste, coarse.

7.20 When assessing whether material is unacceptable, each case will be judged on its merits, taking into account the individual circumstances.

Private Use

7.21 The use of the Trust's Internet or email facilities is not permitted for the pursuit of a private business, or for personal financial gain or gambling.

7.22 Limited private use of the Trust's Internet facilities is permitted. When you are using the Internet at work for private use, you are still identifiable as an employee of The Constellation Trust. You should not therefore engage in any activities that could bring the Trust into disrepute. Personal use of the system, for browsing the Internet should be moderate and in your own time and should not interfere with your work. All Internet use is monitored.

7.23 It is also unacceptable to undertake any activity, which is intended to:

- Corrupt any information held or transmitted on the Internet.
- Detect weaknesses in the security infrastructure (testing firewalls, cracking passwords)
- Disrupt the normal functioning of the Internet or related services (overloading transactions, introducing viruses)
- Damage the reputation of the Trust.

8 MONITORING

8.1 Authorised officers of the Trust and RM may at any time monitor the use of Trust ICT systems and networks. The use of all Trust ICT systems and networks, particularly email and the internet, is subject to recording to detect and deal with abuse of the systems and fault detection. The Trust will not, without reasonable cause, examine any private material that is discovered. Personal data should not be stored on the network and users should not expect 'privacy' in relation to accessing websites, personal email correspondence, personal documents stored on Trust ICT equipment or networks or messages sent via the internet, as these, in principle, are subject to the same checking procedures applied to business related access and email correspondence.

9 PASSWORDS

9.1 The Trust is responsible for ensuring data and the network is as safe and secure as possible. A weak password may result in the compromise or loss of data. As such, all users are responsible for taking the appropriate steps, as outlined below, to create and secure their passwords. The aim of passwords is to protect user's data, children's welfare where access to confidential and sensitive data is allowed and to minimise the risk of unauthorised access to the Trust and school networks. Here are the Trust password guidelines, following:

• Passwords should be a minimum of **14** characters for staff and **8** for students

• Passwords should not contain the user's account name or parts of the user's full name that exceed two consecutive characters.

•They should contain 3 random words that include a **combination** of:

• Uppercase characters (A through Z)

• Lowercase characters (a through z)

• Numbers (0 through 9)

• Symbols (for example , !, $, #, %)

9.2 This follows the guidance from the National Cyber Security Centre: Three random words - NCSC.GOV.UK

9.3 Passwords must NEVER be shared and staff must not write down passwords and other sensitive information.

9.4 Staff should keep passwords secret and protect access to accounts.

10 MONITORING COMPLIANCE WITH AND EFFECTIVENESS OF THE POLICY

10.1 Effectiveness and compliance of this policy will be regularly monitored by the Trust.

11 REVIEW

This Policy and Procedure will be reviewed within one year of the date of implementation.

Appendix 1 Social Media and Acceptable Use Guidance

SOCIAL MEDIA AND ACCEPTABLE USE GUIDANCE

Introduction

It is recognised that staff may be required to use social media for their work, and this guidance includes activities undertaken for work and personal purposes. This guidance applies to all social networking sites, chat rooms, forums, podcasts, blogs, texting, online encyclopaedias with open access (such as Wikipedia) and content sharing sites such as YouTube. Social media can serve as a learning tool where training videos and other materials are made easily accessible to pupils in a user-friendly and engaging way. They can also be a useful tool for schools to communicate key messages to their community and the wider public. However, the open nature of the internet means that social networking sites can leave people vulnerable if they fail to observe a few simple precautions. Social networking websites provide an opportunity for people to communicate 'en masse' and share ideas regardless of geographical distance, however, there is the risk that posts and messages may feel private, when in fact they are in the public domain. This guidance is applicable to all staff, trainees, external contractors, agency workers, volunteers and other individuals who work for, or may provide services on behalf of, the Trust, and references to staff in this guidance refer to all of the above people.

Safeguarding

As detailed within this policy, staff are advised not to communicate with pupils via social network sites, texts or telephone calls, although there may be occasions where it is appropriate and necessary (e.g. where staff and pupils are members of external groups or family and friend networks). If staff are unsure, they should seek advice from their line manager in the first instance. Staff must not share personal contact details with pupils (mobile telephone numbers, non-work email addresses, social networking sites etc.) unless there is a justifiable reason (e.g. family or friend networks or external groups) and any unintended breach must be reported to RM and the user's line manager immediately. If staff receive contact online from a pupil or ex-pupil they should decline the contact, explaining the safeguarding reasons for this, and they should notify their line manager or Designated Safeguarding Lead.

Staff should not post information and photographs about themselves, or school-related matters publicly that they wouldn't want employers, colleagues, students or parents to see.

Confidentiality

Disclosure of confidential information on, or via, social media is likely to be a breach of a number of laws and professional codes of conduct, including:

- the Human Rights Act 1998
- the Health and Safety at Work Act 1974
- the Data Protection Act 2018

Staff should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media. Such laws include (but may not be limited to):

- the Libel Act 1843
- the Defamation Acts 1952 and 1996
- the Copyright, Designs and Patents Act 1988
- the Criminal Justice and Public Order Act 1994
- the Protection from Harassment Act 1997
- the Malicious Communications Act 1998
- the Communications Act 2003

It is crucial that staff ensure they are familiar with the Trust's Data Protection Policy and that they do not breach confidentiality when using social media. Staff must not discuss confidential information relating to the Trust on their personal social media sites or accounts. Photographs, videos or any other images which identify the Trust or school premises, pupils or their families, or staff wearing school logos must not be placed online on any form of personal social media site. Trust and school email addresses and other official contact details must not be used either for setting up personal social media accounts or for the facilitation of communication through such media.

Reputation

The Trust recognises that staff are entitled to make use of social media in a personal capacity away from work. Staff must be mindful that their online actions can potentially cause damage to the reputation of the organisation if they are identified as being employees of, or as having professional links to, the Trust or one of our schools. Staff must therefore ensure that if they engage with social media they must do so sensibly and responsibly. They must be confident that any content, comment or opinion expressed through their personal use of social media will not adversely affect, nor be found damaging to, the reputation or credibility of the Trust, nor otherwise breach any of the Trust's policies. Staff should be aware that, in the event that they access any personal web-based email accounts via their school network, those accounts may be subject to the Trust's internet monitoring. Staff must avoid bringing the Trust into disrepute and must not use any online (or equivalent) facility to attack or abuse colleagues or pupils. Staff are encouraged not to discuss their work on social media, and any views they express should be referred to as their own and not necessarily reflective of their employer's views. Staff must not edit open access online encyclopaedias (such as Wikipedia) in a personal capacity at work, as the source of the correction will be recorded as

the employer's IP address and the intervention will, therefore, appear as if it comes from the Trust/school itself.

Privacy

Staff must ensure their social media accounts do not compromise their professional position and they should ensure that their privacy settings are set correctly. Staff should also be aware that settings can change and they should regularly review their list of friends. Staff are advised to ensure that they set the privacy levels of their personal sites securely and to opt out of public listings on social networking sites in order to safeguard their own privacy. Staff should keep their passwords confidential, should change them often and should at all times be vigilant about what may or may not legitimately be posted online, and should be aware that it is not safe to reveal home addresses, telephone numbers or other personal information online. Staff are encouraged to be mindful of the risk of fraud and identity theft online and are advised to carefully consider the amount of personal information they display, share or reveal online. Staff should always keep their passwords secret and take all necessary measures to protect access to accounts. Individuals should remember that by making use of social media they are effectively placing information within the public domain and cannot be reliant on the belief that supposedly 'private' comments or viewpoints will not gain a wider currency or exposure.

Conduct on social networking sites

When using social media, staff must not do anything that may bring the Trust into disrepute. Staff are encouraged to think about any photos they may appear in and on social media (e.g. they may wish to 'untag' themselves from a photo). If staff find inappropriate references to themselves and/or images of them posted by a 'friend' online, they are encouraged to contact them and the site to have the material removed. Staff are reminded that parents and pupils may access their profile and could, if they find the information and/or images it contains offensive, complain to the Trust. If staff have any concerns about information on their social networking sites or if they are victims of cyber-bullying, they should contact their line manager. Staff must observe all relevant copyright law before posting content that doesn't belong to them.

Caution

Staff are advised to be careful when using social media messaging. For example, as has been found with recent case law, the content of WhatsApp messages can not only lead to the loss of employment but can result in professional disciplinary proceedings against any regulated professionals involved in the behaviour. Case law demonstrates that:

- the private nature of WhatsApp messaging is not a defence
- any WhatsApp group is only as strong as its weakest member (and any persons they are connected with)

- receiving offensive material via WhatsApp, staying in a group in which it is being circulated and not reporting fellow regulated members can all lead to charges of professional misconduct

All social media platforms have reporting/take down processes, therefore if staff come across information on a social media platform they wish to be removed, there are processes for this. However, processes usually involve selecting from a drop-down menu (although some allow a form to be completed with narrative provided). Processes are largely operated by bots, and extreme content is normally automatically taken down. Staff are advised to retain evidence of social media posts that concern them. They are advised to keep a log of problematic social media posts, take screenshots that show the date and time and followers/following (Twitter) or likes/friends/followers (Facebook). For issues with YouTube, staff should download the content recording date, time and number of views. Staff should record all reports or take down requests and set up alerts to enable all content to be monitored and appropriate action taken.

Advice

Relating to Facebook Use

As a minimum, the Trust recommends the following when staff use Facebook:

Privacy Setting

Recommended security level

Send the user messages - friends only

See the user's friend list - friends only

See the user's education and work - friends only

See the user's current city and hometown - friends only

See the user's likes, activities and other connections - friends only

View the user's status, photos, and posts - friends only

Family and relationships - friends only

Photos and videos - friends only

Religious and political views - friends only

Birthday - friends only

Permission to comment on your posts - friends only

Places you check in to - friends only

Contact information - friends only

Only a limited number of Trust staff should have access to using social media sites using their Trust devices.

As a Trust, we do not allow the use of Twitter/X as a social media platform for our schools.

By clicking 'Acknowledge' in your Every account, you agree to the rules detailed in this Acceptable Use Policy and the potential consequences of non-compliance.