IT Policy John O' Gaunt School

Excalibur Academies Trust

September 2020

IT acceptable use policy

1 Introduction: **This policy sets out the requirements with which you must comply when using the Trust's IT and when otherwise using IT in connection with your job including:**

1.1 The Trust's email and internet services.

1.2 Telephones and faxes;

1.3 the use of mobile technology on Trust premises or otherwise in the course of your employment (including 3G / 4G, Bluetooth and other wireless technologies) whether using an Academy, Trust or a personal device; and

1.4 any hardware (such as laptops, printers or mobile phones) or software provided by, or made available by, the Trust.

1.5 This policy also applies to your use of IT off Trust premises if the use involves Personal Information of any member of the Trust community or where the culture or reputation of the Trust or any of its academies are put at risk.

2 **Failure to comply:** Failure to comply will constitute a disciplinary offence and will be dealt with under the Trust's Disciplinary Procedure.

3 **Property:** You should treat any property belonging to the Trust with respect and reasonable care and report any faults or breakages immediately to the ICT coordinator. You should not use the Trust's computers or other IT resources unless you are competent to do so and should ask for training if you need it.

4 **Viruses and other malicious code:** You should be aware of the potential damage that can be caused by computer viruses and other malicious code. You must not introduce or operate any hardware, software, code/script or data, additionally suspicious emails which have not first been checked by the Trust for viruses should not be opened.

5 **Passwords:** Passwords should be long, for example you could use a song lyric or a memorable phrase plus a number. Do not choose a password which is so complex that it's difficult to remember without writing it down. Your password should not be disclosed to anyone else. In addition:

5.1 Your password should be difficult to guess, for example you could base your password on something memorable that no one else would know. You should not use information which other people might know, or be able to find out, such as your address or your birthday.

5.2 You must not use a password which is used for another account. For example, you must not use your password for your private email address or online services for any school account.

5.3 Passwords (and any other security credential you are issued with such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

6 **Leaving workstations:** If you leave your workstation for any period of time you should take appropriate action and, in particular, you should log off or lock your device so that a password is required to gain access again

7 **Concerns**: You have a duty to report any concerns about the use of IT at the Trust to the ICT Coordinator. For example, if you have a concern about IT security or pupils accessing inappropriate material.

8 **Other policies**: This policy should be read alongside the following:

8.1 Code of Conduct;

8.2 data protection policy for Staff;

8.3 information security policy; and

8.4 acceptable use policy for pupils.

Internet

9 **Downloading:** Downloading of any programme or file which is not specifically related to your job is strictly prohibited.

10 **Personal use:** The Trust permits the incidental use of the internet so long as it is kept to a minimum and takes place substantially out of normal working hours. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. If the Trust discovers that excessive periods of time have been spent on the internet provided by the Trust or it has been used for inappropriate purposes (as described in section 14 below) either in or outside working hours, disciplinary action may be taken and internet access may be withdrawn without notice at the discretion of the Principal.

11 **Unsuitable material:** Viewing, retrieving or downloading of pornographic, terrorist or extremist material, or any other material which the Trust believes is unsuitable, at any time, is strictly prohibited and constitutes gross misconduct. Internet access may be withdrawn without notice at the discretion of the Head whilst allegations of unsuitable use are investigated by the Trust.

12 **Location services**: The use of location services represents a risk to the personal safety of those within the Trust community, the Trust's security and its reputation. The use of any website or application, whether on a Trust or personal device, with the capability of publicly identifying the user's location while on Trust premises or otherwise in the course of employment is strictly prohibited at all times.

13 **Contracts:** You are not permitted to enter into any contract or subscription on the internet (including through an App) on behalf the Trust or any of its Academies, without specific permission from the School Business manage/IT Coordinator. This applies both to "free" and paid for contracts, subscriptions and Apps.

14 **Retention periods**: The Trust keeps a record of staff browsing histories for a period of 30 days.

Email

15 **Personal use:** The Trust permits the incidental use of its email systems to send personal emails as long as such use is kept to a minimum and takes place substantially out of normal working hours. Personal emails should be labelled 'personal' in the subject header. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. The Trust may monitor your use of the email system, please see

paragraphs 26 to 30 below, and staff should advise those they communicate with that such emails may be monitored. If the Trust discovers that you have breached these requirements, disciplinary action may be taken.

16 **Status:** Email should be treated in the same way as any other form of written communication. Anything that is written in an email is treated in the same way as any form of writing. You should not include anything in an email which is not appropriate to be published generally.

17 **Inappropriate use:** Any email message which is abusive, discriminatory on grounds of sex, marital or civil partnership status, age, race, disability, sexual orientation or religious belief (or otherwise contrary to our equal opportunities policy), or defamatory is not permitted. Use of the email system in this way constitutes gross misconduct. The Trust will take no responsibility for any offence caused by you as a result of downloading, viewing or forwarding inappropriate emails.

18 **Legal proceedings:** You should be aware that emails are disclosable as evidence in court proceedings and even if they are deleted, a copy may exist on a back-up system or other storage area.

19 **Jokes:** Trivial messages and jokes should not be sent or forwarded to the email system. They could cause the Trust's IT system to suffer delays and / or damage or could cause offence.

20 **Contracts:** Contractual commitments via an email correspondence are not allowed without prior authorisation of the Principal.

21 **Disclaimer:** All correspondence by email should contain the Trust's disclaimer.

22 **Data protection disclosures:** Subject to a number of limited exceptions, potentially all information about an individual may be disclosed should that individual make a subject access request under data protection legislation. There is no exemption for embarrassing information (for example, an exchange of emails containing gossip about the individual will usually be disclosable). Staff must be aware that anything they put in an email is potentially disclosable**.**

Monitoring

23 The Trust regularly monitors and accesses its IT system for purposes connected with the operation of the Trust. The Trust IT system includes any hardware, software, email account, computer, device or telephone provided by the Trust or used for Trust business. The Trust may also monitor staff use of the Trust telephone system and voicemail messages. Staff should be aware that the Trust may monitor the contents of a communication (such as the contents of an email).

24 The purposes of such monitoring and accessing include:

24.1 to help the Trust with its day to day operations. For example, if a member of staff is on holiday or is off sick, their email account may be monitored in case any urgent emails are received; and

24.2 to check staff compliance with the Trust's policies and procedures and to help the Trust fulfil its legal obligations. For example, to investigate allegations that a member of staff has been using their email account to send abusive or inappropriate messages.

25 Monitoring may be carried out on a random basis and it may be carried out in response to a specific incident or concern.

26 The Trust also uses software which automatically monitors the Trust IT system (for example, it would raise an alert if a member of Staff visited a blocked website or sent an email containing an inappropriate word or phrase).

27 The monitoring is carried out by The Trusts IT personal or a company contracted to provide the Trust with ICT services and support. If anything of concern is revealed as a result of such monitoring then this information may be shared with the school Principal and other senior staff where necessary and this may result in disciplinary action. In exceptional circumstances concerns will need to be referred to external agencies such as the Police.

Social media policy

1 **Introduction:** The Trust recognises that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, Bebo, LinkedIn, Twitter, Instagram, Snapchat and all other internet postings including blogs and wikis and other interactive websites. It is also a valuable educational tool.

2 **Purpose:** This policy applies to the use of social media for Trust and your own personal purposes, whether during normal working hours or in your personal time. Its purpose is to help staff avoid the potential pitfalls of sharing information on such social media sites and should be read in conjunction with the acceptable use policy for pupils. This policy is designed for your protection.

3 **IT facilities:** The policy applies regardless of whether the social media is accessed using the Trust's IT facilities and equipment or your personal device.

• **Personal use:** The Trust permits the incidental use of the internet and social media so long as it is kept to a minimum and takes place substantially out of normal working hours. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. If the Trust discovers that excessive periods of time have been spent on the internet provided by the Trust either in or outside working hours, disciplinary action may be taken and internet access may be withdrawn without notice at the discretion of the Principal.]

4 **Guiding principles:** Staff are required to behave responsibly at all times and adhere to the following principles:

4.1 You should not be "Friends" with, "Followers" of, or connect with pupils on any social media or other interactive network. It would be considered inappropriate to connect with pupils on a personal account. Depending on the circumstances, it may also be inappropriate to connect with parents, guardians or carers.

4.2 You must not publish anything which could identify pupils, parents or guardians on any personal social media account, personal webpage or similar platform [• without the prior consent of the Principal in writing. This includes photos, videos, or other materials such as pupil work;

4.3 You must be mindful of how you present yourself and the Trust and its Academies on such media. Staff are entitled to a social life like anyone else. However, the extra-curricular life of an employee at the Trust has professional consequences and this must be considered at all times when sharing Personal Data.

4.4 You should always represent your own views and must not allude to other people's personal views in your internet posts.

4.5 When writing an internet post, you should consider whether the contents would be more appropriate in a private message. While you may have strict privacy controls in place, information could still be shared by others. It is always sensible to consider that any information posted may not remain private.

4.6 You should protect your privacy and that of others by omitting Personal Data from internet posts such as names, email addresses, home or work addresses, phone numbers or other Personal Data.

4.7 You should familiarise yourself with the privacy settings of any social media you use and ensure that public access is restricted. If you are not clear about how to restrict access, you should regard all your information as publicly available and behave accordingly.

4.8 You must not post anything that may offend, insult or humiliate others, particularly on the basis of their sex, age, race, colour, national origin, religion, or belief, sexual orientation, disability, marital status, pregnancy or maternity.

4.9 You must not post anything that could be interpreted as threatening, intimidating or abusive. Offensive posts or messages may be construed as cyber-bullying.

4.10 You must not post disparaging or derogatory remarks about the Trust, its Academies or its Governors, officers, staff, volunteers, pupils or parents, guardians or carers.

4.11 You must not post anything that could be interpreted as glorifying or supporting terrorism, extremism or organisations promoting terrorist or extremist views, or encouraging others to do so.

4.12 You must not use social media in a way which could constitute a breach of any policies contained in this Employment Manual.

5 **Removing postings:** You may be required to remove internet postings which are deemed to constitute a breach of this policy. If you fail to remove postings, this could result in disciplinary action.

6 **Breach:** A breach of this policy may be treated as misconduct and could result in disciplinary action including in serious cases, dismissal.

7 **Monitoring:** The Trust regularly monitors the use of the internet, social media and email systems to check that the use is in accordance with this policy. Please see the IT Acceptable Use Policy for further information on monitoring. If it is discovered that any of the systems are being abused and / or that the terms of this policy are being infringed, disciplinary action may be taken which could result in your dismissal.