CLARIFICATION AND GUIDANCE IN RELATION TO THE ACCEPTABLE USE POLICY (AUP)

CLARIFICATION AND GUIDANCE IN RELATIONTO THE ACCEPTABLE USER POLICY (AUP)

Date of review:	September 2019	Review period:	2 years
Date of next review:	August 2021	Owner:	Board of Directors

All Peterborough Diocese Education Trust's (the Trust) information communication technology (ICT) facilities and information resources remain the property of the Trust and not of particular individuals, teams or departments. By following the Acceptable User Policy (AUP) and this guidance we will help ensure that ICT facilities are used:

· legally;

· securely;

· without undermining the Trust;

· effectively;

· in a spirit of co-operation, trust and consideration for others;

· so that they remain available.

The AUP and this guidance relates to all ICT facilities and services provided by the Trust, although special emphasis is placed on email and the internet. All employees, volunteers, and any other users of our ICT are expected to adhere to the AUP and this guidance.

1. Security

1.1 **Do not disclose personal system passwords or other security details to other employees, volunteers or external agents, and do not use anyone else's log-in; this compromises the security of the Trust.** If someone else gets to know your password, ensure that you change it.

1.2 If you intend to leave your PC or workstation unattended for any reason, you should lock the screen to prevent unauthorised access. Logging off is especially important where members of the public have access to the screen in your absence.

1.3 No pen drives or other storage devices should be used on the Trust's network unless they are used for the purposes of a Trust presentation and are the property of the Trust and secure. Please see paragraph 7 for more detail.

1.4 Do not attempt to gain unauthorised access to information or facilities. The Computer Misuse Act 1990 makes it a criminal offence to obtain

2

unauthorised access to any computer (including workstations and PCs) or to modify its contents. If you do not have access to information or resources you feel you need, contact the Headteacher or the Central Team's Administration Officer, as appropriate.

2. Use of Email

2.1 When to use email:

2.1.1 Use email in preference to paper to reach people quickly (saving time on photocopying / distribution) and to help reduce paper use.

2.1.2 Use the phone for urgent messages (email is a good backup in such instances). Use of email by employees and volunteers of the Trust is permitted and encouraged where such use supports the goals and objectives of the Trust.

2.1.3 However, the Trust has a policy for the use of email whereby employees and volunteers must ensure that they:

2.1.3.1 comply with current legislation;

2.1.3.2 use email in an acceptable way;

2.1.3.3 do not create unnecessary business risk to the Trust by their misuse of email.

2.2 Examples of Unacceptable behavior

2.2.1 Sending confidential information to external locations without appropriate safeguards in place. See paragraph 4 of this document for more details.

2.2.2 Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal.

2.2.3 Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment or bullying.

2.2.4 Using copyrighted information in a way that violates the copyright.

2.2.5 Breaking into the Trust's / academy's or another organisation's system, or unauthorised use of a password / mailbox.

2.2.6 Broadcasting unsolicited personal views on social, political, religious or other non-business related matters.

2.2.7   Transmitting unsolicited commercial or advertising material.

2.2.8   Undertaking deliberate activities that waste employee's effort or networked resources.

2.2.9   Deliberately or recklessly introducing any form of computer virus or malware into the Trust / academy's network.

2.3   Confidentiality

2.3.1   Always exercise caution when committing confidential information to email since the confidentiality of such material cannot be guaranteed.

2.4   General points on email use

2.4.1   When publishing or transmitting information externally be aware that you are representing the Trust and could be seen as speaking on the Trust's behalf. Make it clear when opinions are personal. If in doubt, consult your line manager;

2.4.2   Check your inbox at regular intervals during the working day. Keep your inbox fairly empty so that it just contains items requiring your action. Try to decide what to do with each email as you read it (e.g. delete it, reply to it, save the whole email in a folder, or extract just the useful information and save it somewhere logical);

2.4.3   Keep electronic files of electronic correspondence, only retaining what you need to. Do not print it off and keep paper files unless absolutely necessary;

2.4.4   Treat others with respect and in a way in which you would expect to be treated yourself (e.g. do not send unconstructive feedback, argue, or invite colleagues to make public their displeasure at the actions / decisions of a colleague);

2.4.5   Do not forward emails warning about viruses (they are invariably hoaxes and the IT Manager will probably already be aware of genuine viruses – if in doubt, contact them for advice);

2.4.6   Do not open an email unless you have a reasonably good expectation of what it contains, and do not download files unless they are from a trusted source. Alert the IT Manager if you are sent anything like this unexpectedly; this is one of the most effective means of protecting the Trust / academy against email virus attacks.

2.5   Email signatures

        2.5.1   Keep these short and include your name, title, phone / fax number(s) and website address and GDPR statement.

3.   Use of the Internet

3.1   Use of the Internet by employees and volunteers is permitted and encouraged where such use supports the goals and objectives of the Trust / academy.

3.2   However, when using the Internet, employees and volunteers must ensure that they:

        3.2.1   comply with current legislation;

        3.2.2   use the internet in an acceptable way;

        3.2.3   do not create unnecessary business risk to the Trust / academy by their misuse of the internet.

3.3   Examples of Unacceptable behaviour / use

        3.3.1   Visiting internet sites that contain obscene, hateful, pornographic or other illegal material;

        3.3.2   Using the computer to perpetrate any form of fraud, or software, film or music piracy;

        3.3.3   Using the internet to send offensive or harassing material to other users;

        3.3.4   Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence;

        3.3.5   Hacking into unauthorised areas;

        3.3.6   Creating or transmitting defamatory material;

        3.3.7   Undertaking deliberate activities that waste employees effort or networked resources;

        3.3.8   Deliberately or recklessly introducing any form of computer virus into the Trust's / academy's network.

        3.3.9   Writing, publishing, looking for, bookmarking, accessing or downloading material that might be regarded as obscene or pornographic.

3.4 Chat rooms / instant messaging (IM)

    3.4.1 The use of chat rooms and instant messaging is permitted for business use only. This use must have been agreed with your line manager.

3.5 Webmail

    3.5.1 The use of webmail (e.g. Hotmail, MSN, Google Mail) is not permitted in the organisation unless previously agreed with your line manager.

3.6 Copyright

    3.6.1 Take care to use software legally and in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

    3.6.2 Be aware of copyright law when using content you have found on other organisations' websites. The law is the same as it is for printed materials.

4. Confidentiality

4.1 If you are dealing with personal, sensitive and / or confidential information, then you must ensure that extra care is taken to protect the information.

4.2 If sending personal, sensitive and / or confidential information via email, then the following protocols should be used. If there is any doubt as to the information being sent or the appropriate level of protection required, please check with the Headteacher / a member of the Senior Leadership Team.

    4.2.1 Personal, sensitive and / or confidential information should be contained in an attachment;

    4.2.2 In appropriate cases the attachment should be encrypted, and / or password protected;

    4.2.3 Any password or key must be sent separately and preferably communicated by another means e.g. telephone, text message;

    4.2.4 Before sending the email, verify the recipient by checking the address, and if appropriate, telephoning the recipient to check and inform them that the email will be sent;

    4.2.5 Do not refer to the information in the subject of the email.

5. The Trust's / academy's network

5.1 Keep master copies of important data on the Trust's / academy's network server and not solely on your PC's local C: Drive or portable disks. Not storing data on the Trust's / academy's network server means it will not be backed up and is therefore at risk.

5.2 Ask for advice from the IT Manager if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disk space very quickly and can bring the network to a standstill.

5.3 Be considerate about storing personal (non-Trust/academy) files on the Trust's/academy's network.

5.4 Do not copy files that are accessible centrally into your personal directory unless you have good reason (i.e. you intend to amend them or you need to reference them and the central copies are to be changed or deleted) since this uses up disk space unnecessarily.

6. Personal use of ICT facilities

6.1 Social media

For the purposes of this guidance, social media websites are web-based and mobile technologies which allow parties to communicate instantly with each other or to share data in a public forum. They include websites such as Facebook, Twitter, Google+ and LinkedIn. They also cover blogs and image sharing websites such as YouTube and Flickr. This is not an exhaustive list and you should be aware that this is a constantly changing area.

6.1.1 Use of Social Media at work

6.1.1.1 Employees and volunteers are permitted to make reasonable and appropriate use of social media websites from the Trust's/academy's IT equipment. You should ensure that usage is not excessive and does not interfere with work duties. Use should be restricted to your non-working hours, unless this forms part of your work responsibilities.

6.1.1.2 Access to particular social media websites may be withdrawn in the case of misuse.

6.1.1.3 Inappropriate comments on social media websites can cause damage to the reputation of the Trust / academy if a person is recognised as being an employee or volunteer. It is, therefore, imperative that you are respectful of the Trust's service as a whole including colleagues and competitors.

6.1.1.4 Employees and volunteers should not give the impression that they are representing, giving opinions or otherwise making statements on behalf of the Trust / academy unless appropriately authorised to do so. Personal opinions must be acknowledged as such, and should not be represented in any way that might make them appear to be those of the Trust / academy. Where appropriate, an explicit disclaimer should be included, for example: '*These statements and opinions are my own and not those of the Trust / academy.'*

6.1.1.5 Any communications that employees or volunteers make in a personal capacity must not:

6.1.1.5.1 bring the Trust / academy into disrepute, for example by criticising the Trust / academy or colleagues;

6.1.1.5.2 breach the Trust's Staff Code of Conduct or any other relevant policy;

6.1.1.5.3 breach copyright, for example by using someone else's images or written content without permission;

6.1.1.5.4 do anything which might be viewed as discriminatory against, or harassment towards, any individual, for example, by making offensive or derogatory comments relating to: age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation;

6.1.1.5.5 use social media to bully another individual;

6.1.1.5.6 post images that are discriminatory or offensive (or links to such content).

6.2   Other personal use

6.2.1   Use of facilities for leisure or personal purposes (e.g. sending and receiving personal email, personal phone calls, playing computer games and browsing the internet) is permitted so long as such use does not:

6.2.1.1 incur specific expenditure for the Trust / academy;

6.2.1.2 impact on the performance of your job or role (this is a matter between employee or volunteer and their line manager);

6.2.1.3 break the law;

6.2.1.4 bring the Trust / academy into disrepute;

6.2.1.5 detrimentally affect the network performance by using large amounts of bandwidth (for instance by downloading / streaming of music or videos);

6.2.1.6 impact on the availability of resources needed (physical or network) for business use].

6.2.2 Any information contained within the Trust / academy in any form is for use by the employee or volunteer for the duration of their period of work and should not be used in any way other than for proper business purposes, or transferred into any other format, unless necessary for business use, and with prior agreement of the Headteacher or a member of the Senior Leadership Team.

7. Portable and Mobile ICT Equipment

7.1 This section covers items such as laptops and mobile devices. Please refer to paragraph 4 of this document when considering storing or transferring personal or sensitive data.

7.2 Use of any portable and mobile ICT equipment must be authorised by a member of the Senior Management Team before use.

7.3 All activities carried out on the Trust's/academy's systems and hardware will be monitored in accordance with the general policy.

7.4 Employees and volunteers must ensure that all data belonging to the Trust is stored on the Trust's / academy's network and not kept solely on a laptop. Any equipment where personal data is likely to be stored must be encrypted.

7.5 Equipment must be kept physically secure to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of the car before starting your journey.

7.6 Synchronise all locally stored data, including diary entries, with the central organisation network server on a frequent basis.

7.7 Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.

7.8 The installation of any applications or software packages must be authorised by the IT Manager, fully licensed and only carried out by the IT Manager.

7.9   In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

7.10   Portable equipment must be transported in a protective case if one is supplied.

8.   Remote Access

8.1   If remote access is required, you must contact the IT Manager to set this up.

8.2   You are responsible for all activity via your remote access facility.

8.3   Laptops and mobile devices must have appropriate access protection, i.e. passwords and encryption, and must not be left unattended in public places.

8.4   To prevent unauthorised access to the Trust's / academy's systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone.

8.5   Select PINs that are not easily guessed, e.g. do not use your house or telephone number and do not choose consecutive or repeated numbers.

8.6   Avoid writing down or otherwise recording any network access information where possible. Any information that is written down must be kept in a secure place and disguised so that no other person is able to identify what it is.

8.7   Protect the Trust's information and data at all times, including any printed material produced while using the remote access facility. *(Take particular care when access is from a non-office environment).*

8.8   Users of laptops and mobile devices are advised to check their car and home insurance policies for the level of cover in the event of equipment being stolen or damaged. Appropriate precautions should be taken to minimise risk of theft or damage.

8.9   Care should be taken when working on laptops in public places (e.g. trains) that any employee or pupil details are not visible to other people.

9.   Electronic monitoring

9.1   You may find that you have access to electronic information about the activity of colleagues. Any such information must not be used by unauthorised individuals to monitor the activity of individual employees in any way (e.g. to monitor their working activity, working time, files accessed, internet sites accessed, reading of their email or private files, etc.) without their prior knowledge. Exceptions are:

9.1.1   In the case of a specific allegation of misconduct, when the Headteacher / CEO can authorise accessing of such information when investigating the allegation;

9.1.2   When the IT Manager cannot avoid accessing such information while fixing a problem, but this will only be carried out with the consent of the individual concerned.

10.   Online purchasing

10.1   Any users who place and pay for orders online using personal details do so at their own risk and the Trust accepts no liability if details are fraudulently obtained whilst the user is using the Trust's equipment.

11.   Care of equipment

11.1   Do not rearrange the way in which equipment is plugged in (computers, power supplies, phones, network cabling, modems etc.) without first contacting the IT Manager.

12.   Agreement

All employees, volunteers, contractors or temporary employees who have been granted the right to use the Trust's / academy's ICT systems are required to sign this guidance confirming that they have read it alongside the Acceptable Use Policy (AUP).

Signed:	
Employee /volunteer:	
Date:	