IT and Social Media Policy

In some cases, the Trust provides email, Internet, and IT services for business purposes. The Trust 's systems may only be used by people who are authorised to use them, and who are trained or have been otherwise approved by the Trust to do so, and only for those purposes for which they have been trained and authorised.

Unauthorised use

The use of computer equipment or systems for purposes not directly concerned with the Trust 's business is restricted. You are not permitted to:

1. make excessive use of the Trust 's systems and equipment for non-work purposes;
2. access any restricted parts of the Trust 's network;
3. transmit/disclose confidential, sensitive, or other Trust information to unauthorised parties;
4. view, transmit or download libellous or defamatory material;
5. transmit or disclose system security information or passwords;
6. view, transmits or disclose offensive or non-business related text and/or file attachments, pornographic material, or any material in breach of its Equal Opportunities and Diversity Policy;
7. use the Trust's IT facilities in a way that restricts the services available to others e.g., deliberate, or reckless overloading of access links or switching equipment;
8. delete or modify existing systems, programs, information, or data (except as authorised in the proper performance of your duties).
9. Introduce any harmful or nuisance programs, files, or macros e.g., viruses or worms onto any computer system;
10. take any action to implement or install unauthorised systems or software.
11. download or install software from external sources onto the Company's equipment (as this may contain viruses or other potentially damaging material) – only software that has been approved by the Trust is to be used on its system. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files;
12. use, download, upload or otherwise bring onto the Trust's network, or onto the hard drive of one of the Trust's PCs, games, shareware, or freeware;
13. attach any device or equipment to the Trust's systems without authorisation from Head Office. This includes any USB flash drive, MP3 player, tablet, smartphone, or other similar device, whether connected via the USB port, infra-red connection or in any other way.
14. not view, access, transmit or download illegal, offensive or inappropriate material (for example pornographic or other obscene material or any material in breach of the Equal Opportunities and Diversity Policy).

In the event an employee engages in any unauthorised use, the employee may be subject to disciplinary action under our Disciplinary Policy and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

Access

Employees must not under any circumstances:

1. access any computer or other computer that is not the one allocated to you, unless you have a legitimate reason, or you have been expressly authorised to do so by the Trust;
2. try to gain unauthorised access to any Trust computer system anywhere;
3. allow unauthorised access to occur by their negligence;
4. reveal your password(s) or username to anybody unless there is a genuine business reason;
5. allow other individuals to use their username;
6. violate the privacy of others on the computer systems;
7. leave their workstation logged in and unlocked when unattended;
8. set up any network services e.g., web servers and email servers unless expressly sanctioned by the COO;
9. try to access any information to which you are not permitted access;

In the event an employee engages in any unauthorised use, the employee may be subject to disciplinary action up to and including summary dismissal.

E-mail and electronic communications

The Trust 's systems contain e-mail and electronic communication facilities that is intended to promote effective communication within the organisation on matters relating to business. The e-mail system should be used for that purpose. Brief, occasional personal messages may be sent but employees should adhere to the primary purpose of the system.

E-mail and electronic communications tend to be more informal than written correspondence but should be treated as equivalent to letters. Appropriate standards must be maintained, which should be based on common sense, reasonableness and the professional standards expected from all users by the Trust. E-mails and electronic communications sent externally are no different to letters sent out on the Trust 's headed paper and should be treated in the same regard. A confidentiality notice will automatically be applied to all outbound e-mail. Any inappropriate use of the e-mail and internet facility may result in disciplinary action up to and including summary dismissal (i.e., dismissal without notice).

(a) "Inappropriate" includes (but is not limited to):

- (i) any communication that might bring the professional reputation of the Trust into disrepute, including protected copyright material;
- (ii) the sending of chain letters, junk mail, advertisements other than those which are sent in the course of your duties under your contract of employment, or other trivial content including jokes, quizzes, and video clips;
- (iii) sending abusive material in any e-mail whether business or personal. Examples are e-mails whose content contains any material in any of the following categories:
  - (A) defamatory;
  - (B) offensive or obscene;
  - (C) untrue or malicious;
  - (D) abusive;
  - (E) racist or sexist;

(F) pornographic;
(G) discriminatory;
(H) can otherwise be defined as harassment.

(b) Improper statements contained in e-mails may result in legal action against you or the Trust. It is therefore vital for e-mail messages to be treated like any other form of correspondence and, where necessary, hard copies to be retained. You are reminded that e-mail messages (like any form of recorded material) are disclosable in any legal action commenced against the Trust relevant to the issues set out in the e-mail. Be aware that email messages may have to be disclosed in court proceedings (unless legal privilege attaches to them) or in investigations by regulatory bodies or compensatory authorities. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure.

E-mails do not always reach their destination. If a message is important, make sure you obtain confirmation of receipt. Confidential information should not be sent externally by e-mail or unprotected over the internet as the Trust is unable to guarantee the security of e-mails when sent over a public network such as the internet.

Unless specifically authorised to do so by your manager, under no circumstances may you enter a contractual commitment by e-mail.

If you receive an e-mail message that has been wrongly delivered to your e-mail address, you should notify the sender of the message by redirecting the message to that person. In the event the e-mail message contains confidential information, you must not disclose or use that confidential information.

If you have access to the Internet this is to be used in a manner which is consistent with and appropriate to professional business conduct. In particular, accessing or importing games, pornographic, obscene or other sexually explicit material, information which is or could reasonably be construed as indecent/offensive or in breach of the Trust 's Equal Opportunities and Diversity Policy, material to gain unauthorised access to or for the corruption of the systems, data, networks or computer equipment and illegal material or material for a criminal purpose is strictly forbidden and doing so will be regarded as a disciplinary matter and may lead to summary dismissal.

Monitoring

The Trust's systems enable us to monitor all electronic communications (including emails and instant messages) sent or received by you regardless of the nature of those communications and all material downloaded by you from the Internet. This includes the content of personal folders. For business reasons, and to carry out legal obligations in our role as an employer, use of the Trust's systems including the telephone and computer systems, and any personal use of them, may be continually monitored by automated software or otherwise. Be advised that periodically the Trust will be sweeping email boxes and auditing local and network drives for such material. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes. If you are found in possession of any inappropriate, unlicensed, or otherwise damaging material this may result in disciplinary action.

The company reserves the right to monitor communications facilities for the purposes of:

1. ensuring compliance with this policy as it is set out from time to time;
2. locating and retrieving lost data in the event of hardware or software failure;
3. for checking to see if the Trust 's best practices and standards are being followed; and
4. (on a case-by-case basis) for investigating suspected criminal offences, investigating complaints, countering fraud, obtaining evidence for use in court or tribunal proceedings or detecting other misuse of the Trust 's resources.

Confidentiality
You may not disclose any information of a confidential nature relating to the Trust or any of its subsidiary companies or their business or trade secrets or in respect of which the Trust owes an obligation of confidence to any third party during your employment except in the proper course of your employment or at all after the termination of your employment. You must not download or email Trust information to any storage device or third party including yourself.

All Internet use, whether work related or otherwise, must be in strict compliance with this policy.
These guidelines always apply, not only during working hours.

Trust-owned information held on third party websites
If you produce, collect and/or process business related information in the course of your work, the information remains the property of the Trust. This includes such information as third-party websites such as webmail service providers and social networking sites, such as Facebook and LinkedIn, as well as contacts and data.

Computer Security
The Trust regards the integrity of its computer system is central to the success of the business. The Company's policy is to take any measures it considers necessary to ensure that all aspects of the system are fully protected.

Passwords must be always used and changed regularly. Employees should not select obvious passwords. All passwords must be kept confidential. Employees must not give their passwords to other members of staff or to any person outside the Trust. When an employee leaves the Trust (for any reason), details of passwords must be provided to Head Office and/or all passwords in that department will be changed.
Do not insert unscreened and authorised USB devises into computers.
Documents that contain sensitive personal data should always be password protected.

If you have been issued with a laptop, tablet computer, smartphone, or other mobile device, you must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. You should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

Social Media Policy

Social Media is the social interaction among people in virtual communities and networks. The Trust recognises that Social Media and SMS and MMS communications are a part of ours and our employee's everyday life.

In accordance with the IT Policy, employees cannot update and use Social Media during working time unless as directed by the Trust and in support of recognised business activities.

Use of social media at work
The Trust encourages employees to make reasonable and appropriate use of social media as part of their work. It is an important part of how the organisation communicates and connects with its audience.

Employees may contribute to the organisation's social media activities directly, for example by recording a 'story' or carrying out a 'takeover' for Instagram and Facebook and posting them directly to the channel/s. Direct use of the Trust social media channels must be agreed with the Communications Team.

Employees wishing to contribute to the organisation's social media activities indirectly, for example by writing a blog and creating content (for example: taking photos and video clips whilst out on site) should forward these to the Communication team.

Employees must be always aware that, while contributing to the Trust social media activities, they are representing the Trust.

Employees should not set up online accounts that aim to represent or be associated with the Trust without permission from the Communications Team

Employees who use social media as part of their job must ensure that any communications made through social media must not:

<u>Bring the organisation into disrepute</u>
for example:

- Criticising or arguing with customers, members of the public, colleagues, or rivals.
- Making defamatory comments about individuals or other organisations or groups
- Posting images that are inappropriate or link to inappropriate content

<u>Negatively impact the professionalism of the organisation</u>
for example:

- Creating content that is not factually accurate

<u>Breach confidentiality</u>
for example:

- Revealing sensitive Trust information
- Giving away confidential information about an individual (such as a colleague or customer contact)
- Discussing the Trust's internal workings or its future business plans

Breach copyright, for example by:
- Using someone else's images or written content without permission
- Failing to give acknowledgement where permission has been given to reproduce something

Do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
- Making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age
- Using social media to bully another individual
- Posting images or links to content that are that are discriminatory or offensive

Social media in your personal life
The Trust recognises that many employees make use of social media in a personal capacity and does not seek to overly impact an employee's personal life. However, employees must be aware that they can inadvertently cause damage to the Trust if they are recognised as being an employee of the Trust.

Where an employee's personal social media page is publicly accessible and states that they work for the Trust employees must be mindful of their conduct and content.

Employees must not:

- Bring the organisation into disrepute
- Negatively impact the professionalism of the organisation
- Breach confidentiality
- Do anything that could be considered discriminatory against, or bullying or harassment of, any individual

Protecting Employees online
To protect employees online, any responses to negative comments online must be come from official Trust channels only.

Employees are welcome to engage with the content posted on the Trust social media pages from their personal social media accounts, however, any complaints or potentially contentious and/or negative comments that arise on Trust channels will be managed by the Communications Team.

Employees must not engage individually with negative comments or complaints unless instructed to do so.

The Communications Team will then respond to any such comments from the Trust social channels in an official and consistent manner, ensuring that any public response is made to the organisation, rather than to individual members of staff.

Online harassment/cyber bullying
The rise of online networking and the use of social media has seen the growth of a new type of bullying. Cyber bullying is any form of bullying, harassment, or victimisation online. It can spill from on-screen to off-screen and affect the face-to-face interactions between colleagues at work and away from work.

Cyber bullying can happen in several ways:
- Inappropriate photographs may be posted
- Offensive or threatening comments might be made
- Sensitive personal information could be revealed

This can be done accidentally or vindictively, and cyber bullying can make people feel very distressed and alone.

The Trust is committed to creating a work environment free of harassment and bullying, where everyone is treated with dignity and respect. The problem with online harassment is that social media networking sites and personal smart phones can be used outside of working hours and away from work premises to bully staff.

If an employee feels that they are being harassed online after being involved with the Trust social media pages they should report any such behaviour to their line manager immediately, who will take appropriate action and inform the Communications Team.

Furthermore, abuse of another employees Social Media or message account to cause damage or update anything that could be consider as breaching the Trust's Equal Opportunities and Diversity will be considered to be a disciplinary issue that will warrant disciplinary action up to and including dismissal.

Any misuse of social media should be reported to HR Department. Failure to adhere to the rules and guidance set out in this policy may result in disciplinary action.