IT AND SOCIAL MEDIA ACCEPTABLE USE POLICY

POLICY STATEMENT:

Woodnesborough Community Project (WCP) and Woodnesborough Football Club (WFC), collectively referred to as the Group, use information technology (IT) to enable our volunteers to fulfil the commitments and responsibilities associated with running and promoting our Charity and club. If IT is deliberately or unintentionally misused, the safety and security of data, business continuity and potentially the reputation and financial standing of the Group may be adversely affected. Personal data could also be compromised which could lead to a data security breach and investigation and prosecution by the Information Commissioner's Office.

It is noted that the Group do not provide any IT hardware or telephony to volunteers, so all devices are owned by the volunteers and it is their responsibility to ensure they are secure, have sufficient anti-virus protection etc.

Cybercrime represents a real and immediate threat and can cause significant and far-reaching damage to an organisation. If all volunteers use IT systems correctly and appropriately, the risk of the Group's systems being hacked or held to ransom is reduced.

The manner in which our volunteers conduct themselves in the use of IT is therefore of key importance and all users must ensure that they are compliant with this policy. WCP and WFC will undertake to make users aware of the policy at all appropriate opportunities.

The policy relates to all authorised users of WCP and WFC associated applications, social media accounts and website and covers the following key areas:

- General responsibilities of authorised users
- Emails
- Use of social media
- Software, copyright and downloading
- Consequences of violation

PROCEDURES:

General responsibilities of authorised users

An authorised user (volunteers and users as required) of WCP/WFC applications will have a user account issued to them. In accepting and using their account, users agree to the following general conditions as well as the specific procedures as detailed in this document:

1. All individually allocated user accounts, passwords and email addresses are for the exclusive use of the individual to whom they are allocated. Users must 'lock' their laptops/PCs when they are away from their workspaces to prevent other users from accessing their accounts. Users are personally responsible and accountable for all activities carried out under their user account. The password associated with a particular user account must not be divulged to any other person, other than to designated members for the purposes of system support.

2. Attempts to access or use any user account or email address which is not authorised to the user, are prohibited.

3. Users must use 'strong' passwords in accordance with the protocols advised in cyber security training.

4. Users must take all reasonable precautions to protect their passwords. Individual passwords should not be printed, stored on-line or given to others.

5. Users must alert the club Chairman within 24 hours in cases of theft of, or damage to, hardware and/or the possibility of any breach to the integrity of personal data, IT hardware, software or user accounts.

6. Use of IT systems and hardware must not contravene legislation and must not harm others.

7. Saving personal or sensitive data (special category of personal data) on portable devices (USBs, hard drives, personal 'phones, personal cloud storage etc.) is prohibited. Advice can provide guidance on how to encrypt and store and send personal and sensitive data securely e.g. via a OneDrive link, if normal methods are not usable.

8. If users have any suspicions about any files or email communications e.g. virus or hoaxes, they should not open the file but must take appropriate action to investigate the source to identify if it is from a reliable source and not a virus/hoax – otherwise the item should be deleted. Do not open if unsure.

9. Volunteers must adhere to the requirements and principles of safeguarding when using IT and telephony to communicate with players, supports, users of the Group's facilities. This means not engaging in activity that could compromise professional relations or bring safeguarding into question. For example, Volunteers must not: Divulge personal details such as email addresses and telephone numbers to anyone on a personal level via social media.

10. Facebook, X (formally Twitter) etc. can be used for promotional purposes via official WCP/WFC channels and must adhere to the Social Media Best Practice Guidelines. (X, Facebook, MySpace etc)

11. If a Team or Group associated with WCP/WFC wishes to set up a social media account such as Facebook, X (formally Twitter), WhatsApp or other, permission must be sought from the WFC Chairman. The Admins of these accounts must exercise professional judgement when posting content to internal or external WCP/WFC social media. Content must not be of a nature that will potentially bring the Group into disrepute or be offensive to the viewer. Useful information about the safe and secure use of IT and social networking can be found on the Get Safe Online website and the National Cyber Security Centre.

12. Volunteers must not use personal devices or channels to communicate with players or store information about players e.g. photographs, personal data etc, unless specific permission by the individual (over 18's) or their parent/guardian/carer (for players aged 18 and Under) .

13. When a Volunteer leaves the WCP/WFC, any access to the Group's applications, Social Media accounts or Website must be rescinded ie passwords changed.

Email use

General principles

WCP/WFC's email account is provided for club purposes only. Email accounts and the data stored in them are the property of WCP/WFC. Whilst the Group will take all reasonable steps to respect the privacy of email communications, users should have no expectation of privacy in any email sent or received. Where the content of emails is to be accessed for any of the purposes detailed below, the action must be approved by the Club Chairman following due process. Instances where the Group may have to interrogate emails are as follows.

22. Unexpected or prolonged absence of a member of the Group where not dealing with his or her email in a timely manner adversely affects business operations.
23. To fulfil a legal requirement e.g. a Subject Access Request under Data Protection legislation
24. To assist in disciplinary investigations.
25. To investigate possible criminal activity.

26. Email is recognised as a formal method of communication and has the same status in law as the printed word. Users could incur legal liability for themselves and/or the Group on the basis of information provided or opinions expressed by email. The tone and content of emails should therefore be appropriate, accurate and professional at all times.

27. Reasonable personal use of email by Volunteers is permitted but should not interfere with work obligations. The contents of personal emails must comply with the restriction set out in this policy document.

28. Emails sent outside the Group should include the following Group's standard signature and a notice which will automatically be appended to the following statement:

    "This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you are not the intended recipient or the person responsible for delivering the email to the intended recipient, be advised that you have received this email in error and that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited."

29. Volunteers must be careful not to send emails which disclose the personal data of others to someone who is not authorised to receive it. The content of emails must therefore be checked carefully before they are sent and the recipient's address should be double checked.

30. Volunteers should avoid sending attachments in an email and should link to the source document wherever possible. If a file needs to be transmitted it should be sent via a OneDrive link

31. Emails and attachments which include personal/special category data must not be sent externally via email. A OneDrive link should be used in all circumstances.

32. Emails that are flagged as private or confidential should not be forwarded or shared without the permission of the originator.

<u>Unacceptable use of the email system</u>

42. Using someone else's email address to send messages.
43. Creation or transmission of material which brings the Group into disrepute.
44. Creation or transmission of material that is illegal.
45. The transmission of unsolicited commercial or advertising material, chain letters, press releases or other junk-mail of any kind.
46. The unauthorised transmission to a third party of confidential material concerning the activities of the Group or the personal data of other data subjects.
47. Downloading email attachments from people you don't know - these may contain viruses.

48. The transmission of material that infringes the copyright of another person, including intellectual property rights.
49. Activities that corrupt or destroy other users' data or disrupt the work of other users.
50. Creation or transmission of any offensive, obscene or indecent images, data or other material.
51. Creation or transmission of material that is libellous, abusive or threatening to others, serves to harass or bully others, discriminates or encourages discrimination on the basis of ethnicity, gender, gender identity, sexual orientation, marital status, disability, age, political or religious belief. This includes any material that has, or could be considered to have, the potential to radicalise or incite racial or religious hatred.
52. Activities that violate the privacy of others or unfairly criticise, misrepresent others; this includes copying distribution to other individuals.
53. Creation or transmission of anonymous messages or deliberately forging messages or email header information, (i.e. without clear identification of the sender.)
54. The unauthorised provision of access to WCP/WFC's services and facilities by third parties.

Social media

58. Social media/networking (Facebook, LinkedIn, Twitter, blogs, wikis etc.) can be a valuable tool in communicating WCP/WFC's offer to the wider world however these media may be subject to unwitting abuse by users and it should be noted that the Group can be held vicariously liable for any inappropriate or illegal use of social media.

The following key principles with regard to social media should be observed at all times:

59. Communications must not include anything that could be considered libellous, illegal, offensive, defamatory or that may bring WCP/WFC into disrepute/adversely affect the organisations's reputation.

60. Only Admin's approved by the WFC Chairman can have accounts that can be directly attributed to WFC/WCP ie named Woodnesborough FC in some way or another. Any accounts that have already been setup prior to this policy being created either need to seek permission for the use of the name or the accounts need to be renamed so they cannot be directly linked to WFC/WCP or they must be deleted.

61. WCP/WFC takes bullying and harassment extremely seriously. Volunteers or players who use social media to bully and harass will be subject to the relevant disciplinary procedures.

62. The broadcasting of personal data/information without a person's consent and knowledge is prohibited.

63. Personal views should be qualified by the individual making the statement; it should be made clear that the views are personal and do not reflect the views of WCP/WFC

64. Volunteers should not engage in communications about potentially sensitive or political topics or legal matters relating to WCP/WFC.

65. Any communication via social media must always by respectful and accurate and avoid the possibility of incorrect assumptions being made.

Software, copyright and downloading

66. Copyright applies to all text, pictures, video and sound, including any media sent by email or the internet. Files containing copyright protected material may be downloaded but not forwarded or transmitted to third parties without the permission of the originator or an acknowledgement of the source of the material.

Cloud Computing

Cloud providers are likely to store and move data around multiple servers situated in a number of jurisdictions. This can result in a breach of Data Protection legislation unless there are adequate security measures in place for personal data. Compliance may be achieved if approved contract terms are used with a cloud provider. Under no circumstances must personal or sensitive data as defined in Data Protection legislation be stored in non-Microsoft product cloud-based applications.

When conducting a risk assessment for cloud computing the following aspects should be covered:

79. What "Information Security Standards" does the provider adhere to?
80. Does the cloud provider use third parties to evaluate its own security risks?
81. What identity and access management architecture is in place?
82. How will the cloud provider accommodate the obligations that the institution has with regard to data protection and data retention schedules?
83. Are there clear penalties in the contract for data loss or breach of security and privacy?
84. Can the cloud provider give assurances that information can be taken down without delay from websites or other accessible locations on the instruction of IT services?
85. What planned responses are in place should a service failure occur?
86. Can the cloud provider's facilities be inspected by the institution's IT services?
87. Is data portability part of the service that is provided?
88. Where encryption of data is required is the cloud provider able to facilitate this requirement?

Consequences of violation

Where users are found to violate any aspect of this policy, they will be subject to the immediate withdrawal of user rights and the instigation of disciplinary procedures. Individuals may also be subject to criminal proceedings. WCP/WFC reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of their violation of licensing agreements and/or other contraventions of this policy.