Acceptable IT Use Policy

March 2023

Incorporating:

Appendix 1: Use of Images

Appendix 2: Staff/Volunteer Acceptable Use Agreement/ Code of Conduct

Introduction

Acceptable Use refers to all ICT resources and equipment within Basingstoke Rugby Club ((hereafter referred to as 'the Club') and resources that have been made available to the Club's employees, volunteers and contractors (hereafter referred to as 'individuals') for working remotely or within the club environment. ICT resources and equipment includes club telephones and text systems (including mobile communications), PC's, laptops, mobile devices, webcams, digital video, audio or photographic equipment, computer resources, intranet and virtual learning environments, use of e-mail systems and the internet (fixed and mobile), software (including use of Sage and Stockade), social networking sites, instant messaging services, blogs, storage or recording equipment, and any other electronic or communication equipment used in the course of the employee or volunteer's work. It includes such technologies as provided by the club (used in the club and/or remotely) and those owned by individuals, but brought onto club premises and/or used at home for club business.

This policy applies to:

- all information, in whatever form, relating to the Club's business activities
- all information handled by the club relating to other organisations with whom it deals
- all IT and information communications facilities operated by the Club or on its behalf

The following protocols should be read in conjunction with the club's **Data Protection Policy** and **Social Media Policy**, and relates to other policies including those for Conduct, Child Protection, Safeguarding, Discipline and Complaints.

Individuals with authorized access to club data are given training and guidance to be able to recognise and report potential misuse and to enable them to use software and systems as relevant to their role. Staff are also given guidance in respect of the potential risks and consequences in relation to inappropriate use of their own personal ICT facilities, especially where this use is inconsistent with the expectations of staff working with children and young people.

This policy refers to current advice from the RFU and will be reviewed on a regular basis. It has been agreed by the Club Executive Committee.

Computer Access Control – Individual's Responsibility

Access to the Club's IT systems is controlled by the use of User IDs, passwords, role-assigned access levels and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently individuals are accountable for all actions on the Club's IT systems. Access to Stockade data is authorised to individuals by the Bar Manager via coded tokens and passcodes. Access to GMS data is via specific role-assigned access level.

Individuals must not:

- Allow anyone else to use their user ID/token and password on any Club IT system
- Leave their user accounts logged in at an unattended and unlocked computer
- Use someone else's user ID and password to access the Club's IT systems
- Leave their password unprotected (for example writing it down)
- Perform any unauthorised changes to the Club's IT systems or information
- Attempt to access data that they are not authorised to use or access
- Exceed the limits of their authorisation or specific business need to interrogate the system or data
- Connect any non-Club authorised device to the Club network or IT systems
- Store club data on any non-authorised unprotected equipment
- Give or transfer Club data or software to any person or organisation outside the Club without the authority of the Club. Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

Internet and email

At their discretion, the club gives Committee members and some staff the use of BRFC e-mail accounts to use for all club business as a work-based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed. Staff and volunteers should use their club email for all professional club communication and business. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to the Club in any way, not in breach of any term and condition of employment or this policy and does not place the individual or the Club in breach of statutory or other legal obligations. All individuals are accountable for their actions on the internet and email systems.

Club e-mail and the internet must never be used to communicate anything offensive, defamatory or derogatory. Failure to observe this would be regarded as gross misconduct which may, after proper investigation, lead to dismissal. The deliberate accessing, viewing, downloading or displaying of offensive and inappropriate material, or unauthorised sites, will likewise constitute gross misconduct.

Club emails (created or received) **are disclosable** in response to a request for information under Data protection Act, so e-mail accounts must be actively managed:

- Delete all e-mails of short-term value
- Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- **Keep content professional.** Personal matters should not be discussed using club e-mails

All e-mails should be written and checked carefully before sending, in the same way as a letter written on club headed paper. If personal or sensitive information is contained within the e-mail, the word "CONFIDENTIAL" should be added to the subject line.

The club requires a standard data protection disclaimer to be attached to all BRFC e-mail correspondence. The responsibility for adding this disclaimer lies with the account holder and is available from the Club Honorary Secretary.

When sending an e-mail on behalf of BRFC, staff and volunteers should always use their own assigned club e-mail account so that they are clearly identified as the originator of a message. The number and relevance of e-mail recipients, particularly those being copied, should be restricted to those necessary and appropriate.

Attachments to e-mails should not be forwarded unnecessarily. Whenever possible, a link to the location path to the document is preferable. Attachments from an untrusted source should NEVER be opened, and club accounts must not to be used to store attachments – where relevant, these should be detached and saved to the appropriate shared drive/folder.

Club e-mail should be checked regularly; club accounts must not to be used for personal advertising.

It is the responsibility of each account holder to keep the password secure.
For the safety and security of users and recipients, the club's email system is monitored and recorded by the system Administrator, (Club Honorary Secretary,) to ensure policy compliance and if necessary, e-mail histories can be traced.
However a club e-mail is accessed, (whether directly, through webmail when away from the club or on non-club hardware,) **all the club e-mail policies apply.**

Sending e-mails
If sending e-mails containing personal, sensitive, confidential, classified or financially sensitive data to external third parties or agencies, staff and volunteers must:

- where possible, encrypt or password protect the message and request confirmation of safe receipt
- verify the details, including accurate e-mail address, of any intended recipient of the information
- verify (by phoning) the details of a requestor before responding to e-mail requests for information
- only copy or forward the e-mail to those recipients who are absolutely necessary
- add "CONFIDENTIAL" to the subject line and ensure private content is not disclosed in the subject line
- add a request to recipients that the data is deleted as soon as possible after use

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse
- Use profanity, obscenities, or derogatory remarks in communications
- Access, download, send or receive any data (including images) which the Club considers offensive in any way including sexually explicit, discriminatory, defamatory or libellous material
- Use the internet or email to make personal gains or conduct a personal business
- Use the internet or email to gamble
- Use the email systems in a way that could affect its reliability or effectiveness, for example, distributing chain letters or spam
- Place any information on the Internet that relates to the Club, alter any information about it, or express any opinion about the Club unless they are specifically authorised to do this
- Send unprotected sensitive or confidential information externally
- Make official commitments through the internet or email on behalf of the Club unless authorised to do so
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval
- In any way infringe any copyright, database rights, trademarks or other intellectual property
- Download any software from the internet without prior approval of your line manager
- Connect Club devices to the internet using non-standard connections

Clear Desk and Clear Screen Policy
In order to reduce the risk of unauthorised access or loss of information, the Club enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended
- Care must be taken to not leave confidential material on printers or photocopiers

- All business-related printed matter must be disposed of using confidential waste bins or shredders

Social Media and the Internet, including Website Blogs, Facebook and Twitter

Whilst any members of club staff/volunteers may be involved in drafting material for the club website or social media platforms, staff must ensure that they follow appropriate and agreed approval processes before uploading material.

For further details, see **BRFC Social Media Policy**:
http://www.basingstokerfc.com/Media/BasingstokeRFCLtd/BRFC/Policies/BRFC%20Social%20Media%20Policy%202019.pdf

Facebook, Twitter and other forms of social media are increasingly becoming a widely used part of our daily lives, but the club recognises the risks associated with use of the Internet and social media and regulates their use to ensure this does not damage the club, its staff and the community it serves. To this end, we encourage staff/volunteers to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

Risks include:

- cyber bullying by others
- access to inappropriate material
- offending behaviour toward staff members by others
- other misuse by staff including inappropriate personal use
- inappropriate behaviour, criticism and complaints from external sources
- loss or theft of personal data
- virus or other malware (malicious software) infection from infected sites
- disclosure of confidential information
- damage to the reputation of the club
- social engineering attacks - i.e. the act of manipulating people into disclosing confidential material or carrying out certain actions
- civil or criminal action relating to breaches of legislation
- staff members openly identifying themselves as club personnel and making disparaging remarks about the club and/or its policies, about other staff members or volunteers, players or other people associated with the club

The Club has a duty to provide a safe working environment for staff and volunteers, free from bullying and harassment. If a staff member uses any information and/or communications technology, including email and social networking sites, to make reference to people working at or for the club, or players at the club, or people receiving services from the Club then any information posted must comply with all relevant professional Codes of Practice and the club's Acceptable Use Policy. Individuals are advised that inappropriate communications that come to the attention of the club can lead to disciplinary action, including dismissal.

Staff must ensure that they use the Internet sensibly, responsibly and lawfully and that use of the Internet and social media does not compromise club information or computer systems and networks. They must ensure that their use will not adversely affect the club or its business, nor be damaging to the club's reputation and credibility or otherwise violate any club policies or RFU Regulations. In particular:

- any publication on behalf of the club must comply with all of the requirements of the **Data Protection Act 1998** and by the **GDPR May 2018** and must not breach any common law duty of confidentiality, or any right to privacy conferred by the **Human Rights Act 1998**, or similar duty to protect private information.

- the tone of any publication on behalf of the club must be respectful and professional at all times, and material must not be couched in an abusive, hateful, or otherwise disrespectful manner
- material published must not risk actions for defamation, breach copyright, or be of an illegal, sexual, discriminatory or offensive nature; it should always be truthful, objective, legal, decent and honest
- if social media is used with players under the age of 18, staff/volunteers must ensure that the site's rules and regulations allow the age group to have accounts and that the parents are informed of its use
- staff members/volunteers must not use the Internet or social media if doing so could pose a risk (e.g. financial or reputational) to the club, its staff or services
- users must not create, download, upload or transmit any images, data or other material which is:
    - obscene or indecent, or capable of being resolved into obscene or indecent images or material
    - sexist, racist, offensive or otherwise unlawful
    - designed or would be likely to annoy, harass, bully, inconvenience or cause anxiety to others
    - unsolicited commercial or bulk web mail, chain letters or advertisements
    - music, images, photos and video that would be in breach of consent, copyright or licensing arrangements, or where copyright or ownership cannot be determined

Personal use of Internet and social media

- the club is not liable for any financial or material loss to an individual user in accessing the Internet for personal use
- volunteers working with children at the club who are using electronic devices with their players should ensure that there is no inappropriate content on any of these pieces of equipment and ensure that they are not accessed by players under the age of 18 at any time.
- in accordance with GDPR, staff/volunteers must never give out personal details of others, such as home address and telephone numbers, without authorisation

Safe Use of Images

(and see Appendix 1: Use of Images)

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the club community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of players under the age of 18), and in accordance with RFU Safeguarding Regulation 21, the club permits the appropriate taking of images
- Where the club proposes to use photos for publication, this is always in accordance with the club's **Data Protection Policy (http://www.basingstokerfc.com/Media/BasingstokeRFCLtd/BRFC/Policies/BRFC%20DP%20PrivacyPolicy_Neutral.pdf)**
- For video used for performance analysis, see additional information at Appendix 1 below.

Publishing Images of players under the age of 18:

Where given, such consent is considered valid for the entire period that the child attends this club unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the club.
If under the age of 18, players' names will not be published alongside their image and vice versa. Likewise, players' full names, e-mail and postal addresses will not be published.
Before posting a player's image on the Internet or sharing it with others, a check needs to be made to ensure that permission has been given for this to be displayed.

Video Conferencing

- Permission must be sought from parents/carers if children are involved in video conferences
- All players under the age of 18 must be supervised by a member of staff/DBS checked volunteer when video conferencing
- No part of any video conference may be recorded in any medium without the consent of those taking part

Note: the club uses CCTV for security and safety. Please refer to the section on CCTV in the **BRFC Data Protection Policy** (**http://www.basingstokerfc.com/Media/BasingstokeRFCLtd/BRFC/Policies/BRFC%20DP%20PrivacyPolicy_Neutral.pdf**)

Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Equipment and media taken off-site must not be left unattended in public places and not left in sight inside a car
- Laptops/mobile devices must be carried as hand luggage when travelling
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption
- The use of Clubs computer equipment at home, including monitors and printers is only allowed with the approval of the Honorary Secretary. Individuals' own devices may be used remotely or on site to access club data under the guidance set out herein.

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only Club authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data. Where staff or volunteers are using external drives/USB sticks for club activity, they must ensure that they have undertaken appropriate virus checking on their systems.

Software

Employees must use only software that is authorised by the Club on Club's computers. Authorised software must be used in accordance with the software supplier's licensing agreements. Installation of any software on Club computers must be approved by the Honorary Secretary.
Individuals must not:

- Store personal files such as music, video, photographs or games on Club IT equipment

Virus Detection and Protection

The Club has implemented centralised, automated virus detection and virus software updates. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved Club anti-virus software and procedures

Telephony (Voice) Equipment

Use of Club voice equipment is intended for business use. Individuals must not use the Club's voice facilities for sending or receiving private communications on personal matters, except in exceptional, authorised circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications.

Individuals must not:

- Use the Club's voice equipment for conducting private business
- Make hoax or threatening calls to internal or external destinations
- Accept reverse charge calls from domestic or International operators, unless it is for business use

Actions upon Termination of Contract/Vacation of Volunteer Role

All Club equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to the Club at termination of contract or cessation of volunteer role. All Club data or intellectual property developed or gained during the period of employment (paid or voluntary) remains the property of the Club and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering

All data that is created and/or stored on Club computers is the property of the Club and there is no official provision for individual data privacy, however wherever possible the Club will avoid opening personal emails, and all new role holders with access to data will be briefed in accordance with the requirements of the Data protection Act and the requirements of the GDPR.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. The Club has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse. Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the GDPR (2018), the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

This policy must be read in conjunction with:

- Computer Misuse Act 1990
- Data Protection Act 1998
- GDPR May 2018

It is the responsibility of all individuals within BRFC to report suspected breaches of security policy or any concerns about the security of the ICT system without delay to their line management or the Honorary Secretary. All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Club disciplinary procedures.

Staff/volunteers must ensure that their use of the club's ICT facilities does not compromise rights of any individuals under the **Data Protection Act 1998** and by the **GDPR May 2018**. This is particularly important when using data off site, and downloaded electronic data must only be taken off site in a secure manner, either through password protected or encrypted devices. This is also particularly important when communicating personal data via email rather than through secure systems. In these

circumstances, staff must ensure that they have the correct email address and have verified the identity of the person that they are communicating the data with.
Staff must also ensure that they do not compromise any rights of individuals and companies under the laws of Copyright through their use of ICT facilities.

Unacceptable Use

Club systems and resources must not be used under any circumstances for the following purposes:

- to communicate any information that is confidential to the club or to communicate/share confidential information which the member of staff/volunteer does not have authority to share
- to present any personal views and opinions as the views of the club, or to make any comments that are libellous, slanderous, false or misrepresent others
- to access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene or discriminatory material
- to communicate anything via ICT resources and systems or post that may be regarded as defamatory, derogatory, discriminatory, harassing, bullying or offensive, either internally or externally
- to upload, download, post, email or otherwise transmit or store material that contains software viruses or any other computer code, files or programmes designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment
- to collect or store personal information about others without direct reference to the **Data Protection Act 1998** and by the **GDPR May 2018**
- to use the club's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of an authorised project
- to undertake any activity (whether communicating, accessing, viewing, sharing, uploading or downloading) which has negative implications for the safeguarding of children and young people

Any of the above activities are likely to be regarded as gross misconduct, which may, after proper investigation, lead to dismissal and/or prosecution. If employees are unsure about the use of ICT resources including email and the intranet, advice should be sought from an Officer of the Club.

If any member of staff or volunteer has genuine concerns about any abuse or inappropriate use of ICT resources, virtual learning environments, camera/recording equipment, telephony, social networking sites, email or internet facilities or inappropriate communications, whether by players, club staff or colleagues, should alert the Data Officer, Club Chair or Club Hon Sec to such abuse. If any matter concerns child safety, it should also be reported to the Club Safeguarding Officer (CSO.)
See also **Club Code of Conduct**,
http://www.basingstokerfc.com/Media/BasingstokeRFCLtd/BRFC/Policies/BRFC%20Code%20of%20Conduct.pdf

Appendix 1:
Use of Images

Policy and Guidance on the use of Photographs, Images and Videos

1. The RFU and Basingstoke RFC positively encourage parents and spectators to take photographs of participants involved in rugby union to celebrate the ethos and spirit of the sport. Basingstoke RFC does not prevent parents from taking pictures of or filming their children. These are normal family practices and help mark milestones in a child's life.

2. However, there may be circumstances where taking a photograph of a child might not be acceptable. Photos and video clips can make any child featured vulnerable to grooming if information about the child (name, address, activities or interests) is also disclosed. Furthermore, posting an image on the website carries a risk that the image could be taken and adapted for an inappropriate use. Any photograph (digital or printed) which is produced and released into the public domain including closed parent groups, may be misused by anyone and once this has been done, control has been lost. In this day and age when it is so easy to upload or email a photograph within seconds of it being taken Basingstoke RFC wishes to ensure that photography and video footage use within the club is undertaken appropriately.

3. The introduction of proportionate controls on the use of photographic equipment (cameras, videos, including mobile phones) is an element of general safeguarding good practice at our club. It is not the intention of Basingstoke RFC to prevent photographs being taken for legitimate purposes.

4. Some people may use sporting events as an opportunity to take inappropriate photographs or film footage of young people. We require all coaches, parents, players, staff, members and volunteers to be vigilant about the possibility of this. These individuals may attend the club allowing people to presume they are related to a child involved. It is also the possible that if a picture and name was placed in the local paper, on the Club Website or in a Club Publication the information could be used as a 'grooming' tool.

5. The club respects that there may be reasons why individuals do not wish their child's photograph to be taken by someone they do not know personally, i.e. estranged parents looking to gain access to a child. For some children – particularly Children in Care, there may be legal and robust constraints on them being photographed and identified. In this instance, everyone involved in the club and our sport must respect these decisions and adhere to these individuals' wishes.

6. Basingstoke RFC uses the following guiding principles relating to the use of cameras during matches, training sessions and other club occasions:
   - Photographs / images /videos are not to be taken at matches or training without the prior permission of the parents/carers of the children. This permission can be given by proxy by the coach of each team only after parental consent for this has been granted. **The coach must arrange this prior to attending matches**.
   - This permission will form part of the player affiliation process and will be renewed at the start of each season. Parents are asked to update their family registration details on the RFU's Games Management system providing these relevant permissions each season.
   - If photographic consent has NOT been given for a child on the player's affiliation, then the Lead Coach / Team Manager will be made aware and it is their responsibility to

ensure that photos of that particular child are not taken, with support from the Club's Safeguarding Team.

- Ideally photographs should be of the activity or team, not of one individual.
- The children should be informed that a person will be taking photographs.
- All children should be informed that if they have concerns they can report these to their coach, team manager or the Club's Safeguarding Team.
- Photographs must provide a positive image of the young people, the Club and the game. Images of errors, injuries and altercations could bring the Club into disrepute.
- Parents should be made aware if a film is being taken to be used as a coaching aid. Clubs and CBs should ensure that any footage will be carefully monitored and stored securely.
- Where photos/videos have been taken, notification must then be provided to parents/coaches of the intended use/sharing/storage conditions etc. according to template at Annex A
- Teams are advised not to post images – either officially or unofficially - on social networking sites which young people can access and tag, thereby revealing more personal information about themselves.
- Concerns regarding inappropriate or intrusive photography should be reported to the Club Safeguarding Team and recorded in the same manner as any other child protection concern.
- Children must be appropriately dressed when being photographed. It is never acceptable to capture any images in changing rooms, showers or at any time when players are dressing. Only use images of young people in appropriate kit (training or playing). Images should be neither sexual, of an exploitative nature nor open to misinterpretation or misuse.

7. Basingstoke RFC recommends the following guiding principles for matches/tournaments/festivals/ events/competitions:
    - Set up a camera registration book for parents to complete before the event begins. Parents should be aware that they may be asked to register their intention to take photographs.
    - All participants in matches/tournaments /festivals /events must adhere to the appropriate guidelines relating to publishing of images at that specific event.
    - Personal information which can lead to a child being identified must never be used. If the player is named, try to avoid using their photograph. On very rare occasions where is necessary to name a child, ensure you have written parental consent and have informed the parents as to how the image will be used. This is particularly important when issuing press releases and match reports.
    - Basingstoke RFC will ensure that parental consent is obtained for photographs to be taken whilst a child is either at the club or away fixtures. This is done easily at the beginning of the season though membership registration.
    - Basingstoke RFC recommends that confirmation is obtained from each club present that parental permission has been given for all the children participating. If there is a child who is the subject of a court order who should therefore not have their photograph taken, this should be addressed before the event.
    - The reporting of inappropriate use of images of children is strongly encouraged. If anyone is concerned they must report their concerns to the CB (Constituent Body Hampshire) Safeguarding Manager or Club's Safeguarding Team.

Commissioning Professional Photographers & the Local Media

8. If the club commissions professional photographers or invites the press to cover an activity, the club will ensure everyone is clear about each other's expectations. Basingstoke RFC with the guidance of the CB will:
    - Ensure that the photographer has been appropriately vetted prior to the event.
    - Provide a clear brief about what is considered appropriate in terms of content and behaviour.
    - Inform them of the club's commitment to safeguarding children. Establish who will hold the recorded images and what they intend to do with them.
    - Issue the professional photographer with identification, which must be worn at all times.

9. Use of images of children, for example on Club websites, in the media, match reports or in club programmes or publications handbooks.
    - The club will always for parental permission to use their child's image and wherever possible show the image to the parents and young person in advance. This ensures that they are aware of the way the image will be used to represent Rugby Union and the Club
    - Ask for the young person's permission to use their image. This ensures that they are aware of the way the image is to be used to represent Rugby Union and the Club
    - If a photograph is used, the club will avoid naming the child. Photographs could be captioned - For example, "Another try for the Basingstoke winger", or "a Basingstoke RFC player scores a good try".

Using Video as a coaching aid

10. There is no intention on the part of the Basingstoke RFC or the RFU to prevent Club Coaches using video equipment as a legitimate coaching aid. However, players and parents/carers must be made aware that this is part of the Coaching programme. The Club and CB will ensure that any footage or material taken in connection with coaching will be carefully monitored, stored securely and deleted /destroyed when a parent requests this, or when the material is no longer needed.
11. Parents/carers and children must have provided written consent for the use of photography and video analysis as described above.
12. Use of video analysis tools (VEO)
    Sharing video analysis – please note there are strict rules about onward sharing:
        - Team Managers to check if there are any vulnerable individuals in their team before taking the option to use video analysis tools such as the VEO system.
        - When you use the VEO system, it uploads directly to secure VEO servers and clears camera storage automatically. VEO footage must **NOT** be downloaded to private devices.
        - Users are prohibited from player tagging or player tracking when sharing with others. Use ball tracking mode only.
        - Sharing to a FB page (even a closed, private group) and/or via an email link is **prohibited**, since for VEO the settings must be public, therefore there are no onward sharing/privacy controls. Sharing to a private u-tube channel to which only players are subscribed or sharing live using club screen equipment may be the best options.
        - The "Share with opponent" link should ONLY be used with **adult video analysis** if requested by the opposition. Then you can review who its shared with and revoke when you want to: sharing youth VEO footage with opposition is **not permitted** as we have no control over their onward sharing.
        - Users must sign an agreement to agree to T&C's as part of their instructions and permissions to use (see Appendix 2).

- Note: Administrators can see **all** recording and **all** teams – full access. Editor can edit, Viewer can just watch, but note that Players, editors and admins can all tag a player….when sharing with players, please instruct them **NOT** to tag players.

This policy has been be adopted in accordance with the club constitution.

Signed:

Date:

ANNEX 1

BRFC GDPR Data Sharing Template:

Dear Parents

Thank you for giving your consent to *take photos/video/collect data** from *yourselves/the players**(delete as applicable)*.

Now that we have collected this data, we would like to let you know the following details about how we are intending to use it, store it, share it, and ultimately delete it, and to give you a chance to feed back to us before we go ahead with our plans, in accordance with our Data Protection Policy (which can be found at http://www.basingstokerfc.com/Media/BasingstokeRFCLtd/BRFC/Policies/BRFC%20DP%20DraftPrivacyPolicy_Neutral.pdf)

Data Description:	
Data file format:	
Data file size:	
Data location:	
Data Scope:	
Intended data Use:	
Sharing method:	
Shared duration:	
Data Retained until:	
Deletion:	

Please contact the Team manager on: (*insert email/mobile)*

with any queries or concerns within the next 48hours, after which we intend *(please state intention eg, to share the video via password protected link, see example below)* as detailed above.

Kind regards,

ANNEX 2

BRFC GDPR Data Sharing Template (example):

Dear Parents

Thank you for giving your consent to *take photos/video/collect data** from *yourselves/the players**(delete as applicable)*.

Now that we have collected this data, we would like to let you know the following details about how we are intending to use it, store it, share it, and ultimately delete it, and to give you a chance to feed back to us before we go ahead with our plans, in accordance with our Data Protection Policy (which can be found at http://www.basingstokerfc.com/Media/BasingstokeRFCLtd/BRFC/Policies/BRFC%20DP%20DraftPrivacyPolicy_Neutral.pdf)

Data Description:	*?? minute video file/VEO footage of ……..Age Group Boys/Girls vs ….. RFC Age Group Boys/Girls match on date xxx*
Data file format:	*e.g. MP4 file, video stored on VEO website cloud*
Data file size:	….GB
Data location:	*Transferred from video recording device via smartcard to Microsoft Personal One Drive (by ……)*
Data Scope:	*Identifiable video images of ……and ……. players, coaches, supporters and game officials.*
Intended data Use:	*Game analysis for developmental purposes by DBS checked Coaching Staff & Officials, plus players from …. and ….* *Parent viewing* *GCSE PE assessment purposes*
Sharing method:	*Password protected shared access URL – access controlled to parent group only, no sharing on private social media please*
Shared duration:	*Link will be available to view for 28 days from agreement*
Data Retained until:	*3rd May 2020*
Deletion:	*At end of retention period*

Please contact the Team manager on: *(insert email/mobile)*

with any queries or concerns within the next 48hours, after which we intend *(please state intention, eg to share the video via password protected link* as detailed above.

Kind regards,

Name

Appendix 2:
Staff/Volunteer Acceptable Use Agreement/ Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life. This agreement is designed to ensure that all BRFC staff and volunteers are aware of their professional, social and legal responsibilities when using any form of ICT on behalf of, or during the work activities for, the club. All staff and club volunteers should sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with the Data Officer, Chair or Honorary Secretary.

- I appreciate that ICT includes a wide range of systems, including mobile phones, smart watches, personal digital assistants, cameras, email, use of social networking, internet and that ICT use may also include personal ICT devices when used for club business. I will only use the club's email / Internet / Social Media platforms and any related technologies for professional purposes or for uses deemed acceptable by the Club
- I understand that it may be a criminal offence to use the club ICT system for a purpose not permitted or to access inappropriate content, including accessing, viewing, uploading, communicating, distributing and downloading material which is pornographic, illegal, offensive, defamatory, derogatory, harassing or bullying
- I understand that I must not communicate information which is confidential to the club or which I do not have the authority to share
- I understand that club information/communication systems and hardware may not be used for personal financial gain, gambling, political activity, advertising or illegal purposes
- I understand that my use of club information systems and email may be monitored and recorded, subject to the safeguards outlined in the policy to ensure policy compliance. The club may also exercise its right to intercept email and to delete inappropriate materials where it believes unauthorised use of the club's ICT systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, images or sound
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own
- I will ensure that personal data is stored securely and is used appropriately whether in the club, taken off the club premises or accessed remotely. I will not routinely keep personal data on removable storage devices. If I take personal or sensitive data off-site, it will be password protected/encrypted and removed/returned after use
- I understand that images/videos of players and/ or staff or volunteers will only be taken, stored and used for professional purposes in line with club policy and with the **prior consent of the parent, carer or staff member**. I confirm that I have checked with the Club Data Officer/Club Safeguarding Officer that such consents are in place for all involved. I have read and understood the BRFC Acceptable Use Policy.
- I will respect copyright, intellectual property and data protection rights
- I will report any incidences of concern regarding children's safety to the CSO
- I will report any incidences of inappropriate use or abuse of ICT and inappropriate electronic communications to the Data Officer or to an Officer of the Club
- I will ensure that any electronic communication undertaken on behalf of the club, including email and instant messaging are compatible with my professional role within the club and that messages do not present personal views or opinions and cannot be misunderstood or misinterpreted. I will ensure that my online activity, both in and outside of the club, will not bring the club, my professional reputation, or that of others, into disrepute

Name (block capitals) ……

Signature……Date……