BEAUDESERT PARK SCHOOL

ACCEPTABLE USE POLICY & CODE OF CONDUCT FOR ICT AND SOCIAL MEDIA

INTRODUCTION

Beaudesert Park School ("the School") aims to educate staff, pupils and the wider community to use ICT effectively to support and develop learning. ICT includes a wide range of systems such as mobile phones, tablets, digital cameras, and email. ICT use may also include personal use of ICT devices when used for school business.

This Policy also covers the use of social media sites by staff and pupils, as well as by the wider School community, including parents, governors and other volunteers.

This Acceptable Use Policy & Code of Conduct for the use of ICT and Social Media ("AUP Policy") should be read in conjunction with the School's Anti-Bullying Policy and the Promoting Welfare and Safeguarding Policy.

STATEMENT OF INTENT

This Acceptable Use Policy is intended to ensure:

- That staff are responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- That School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk; and
- That staff are protected from potential risk in their use of ICT in their everyday work.
- That social media sites are not used inappropriately by staff and pupils as well as by the wider School community, including parents, governors and other volunteers.

PRINCIPLES OF ICT PROVISION

Equal Access to ICT Services
The School's policy is to use and develop opportunities provided by ICT to benefit the school community. All members have the right to equal access to resources. ICT facilities can be booked by staff for lessons and after-school use. Uses such as approved

class work/homework have priority over other uses, such as browsing the internet. Pupils may be asked to remove files if total system storage space becomes low. It is each individual's responsibility to organise their user area and to make private files secure.

The Right to Privacy in Electronic Communication and Work
Files may be accessed by the ICT Support Team as part of normal maintenance. This maintenance may include spot checks to ensure that inappropriate or copyrighted materials are not being kept in private folders. Personal files and e-mails will be accessed if there is a legitimate reason to do so and only with senior level approval and such access is tracked.

Safety from Harassment
If a person feels harassed or threatened by somebody on the school network or internet, they should bring it to the attention of a member of staff or their line manager immediately. Misuse of the e-mail system can result in an e-mail ban as well as further action being taken.

Intellectual Freedom
Viewpoints will not normally be restricted on the network, however use of unacceptable language or inappropriate content will be identified by our monitoring system and action will be taken.

RESPONSIBILITIES OF USERS

Never share a password with anyone
Access to the School network requires entry of a User ID which is unique to the individual and a password which is chosen by the user. All users have full responsibility for the use of their account, and will be held responsible for any policy violations that are traced to their User ID. If the user feels that their password has been compromised or someone else may have access to their password, it is their responsibility to arrange for it to be changed immediately via IT Support Team (the Library staff or designated teachers). Teachers can change passwords via tools provided by ICT Support where appropriate.

Under the Computer Misuse Act 1990 it is illegal to either obtain or use someone else's password to gain access to their user area or e-mail without their permission or knowledge. It is also illegal under this Act to access areas of computers or networks for which you have no authority.

Use of equipment
Users should take due care when using ICT equipment to ensure that no damage is caused. Whilst it is recognised that some wear and tear to the equipment will occur, wilful damage to any school equipment, for example through moving or disconnecting mice or keyboards, will involve sanctions such as reimbursement.

Use of the Network
Users should not knowingly interfere with the performance of the network therefore electronic chain letters, large graphics and downloaded software are prohibited for this reason. Circumventing the School network by use of proxy sites or unsecured local

networks is prohibited. Uploading of third party data or software onto the School network is not allowed unless previously agreed with the IT Manager. This is to ensure that no viruses are brought into the School system and the network and systems can be fully supported.

Respecting Copyright Law
Ownership of text, music, software and other media is protected to the full extent of the law. No copying of protected work is allowed on the School network. It is the user's responsibility to comply with the Copyright Law. Accreditation should always be given for use of any third party content.

Behaviour on the Network/Internet Access
Under no circumstances should users access inappropriate images nor should any material which is likely to be unsuitable for use within the School be viewed, uploaded or downloaded. Using the internet to download, send, print, display or gain access to materials that are unlawful, obscene or abusive is not permitted. The use of social messaging and chat rooms is prohibited except for valid educational use.

Printing
Print facilities are provided throughout the School for School related work.
Documents should be printed in black and white unless printing in colour is essential.
These facilities should not be used for printing for private use.

Children's use of mobile devices (eg. iPods)
Children are responsible for the content on their mobile device. The content must be appropriate for their age range (eg. film rated and game rated). If staff have concerns it is within their rights to check mobile devices for unsuitable material and to confiscate the device if necessary.

In the boarding house

Mobile devices are allowed but these must remain in the dormitories at all times. If discovered outside of the boarding house the devices will be confiscated. Photography and video with mobile devices is strictly forbidden.

During the day

Mobile devices are not allowed on School trips (eg. match journey/ theatre trip). Only in exceptional circumstances will permission be given by staff.

USE OF SOCIAL MEDIA SITES

Pupils are not allowed to access social networking sites whilst at school.

USE OF PERSONAL SOCIAL MEDIA SITES BY EMPLOYEES

It is important that staff protect their professional reputation and that of the School, by ensuring that any use of personal social networking sites is in an appropriate manner, at all times.

Staff will be advised as follows:

- That their privacy settings on all personal social media accounts must be set to the highest possible level.
- That they do not conduct or portray themselves, or allow friends to portray them, in a manner which may:
    - Bring the School into disrepute;
    - Lead to parental complaints;
    - Be considered derogatory towards the School and/or its employees;
    - Be considered derogatory towards pupils, parents or governors
    - Bring into question their appropriateness to work with children
- That they should not form online friendships or enter into communication with parents via social media sites as this could lead to professional relationships being compromised.
- That they do not form online friendships or enter into any online communication with pupils as this could lead to professional relationships being compromised, and/or safeguarding allegations being raised.
- That any communication received from pupils or 'friend requests' on any personal social media sites must be reported to the School's designated Safeguarding Lead responsible for child protection.
- That they should not make any posts or comments that refer to specific, individual matters related to the School and members of its community on any social media accounts.
- That if their use of social media/networking sites contravenes this policy, they may be subject to disciplinary action.

Inappropriate use of social media by staff should be referred to the Headmaster in the first instance.

USE OF SCHOOL SOCIAL MEDIA SITES BY STAFF

All social media sites used by the School must be approved by the Headmaster in advance.

Individual names of children may not be used. Photos of children who are on the Photographic/Recordings exclusion list may not be used.

Staff must make sure that they do not post anything on a social media site used by the School that may:

- Bring the School into disrepute
- Lead to parental complaints
- Be considered derogatory towards the School and/or its employees
- Be considered derogatory towards pupils, parents or governors
- Bring into question their appropriateness to work with children

Inappropriate use of such social media sites by staff should be referred to the Headmaster in the first instance.

Inappropriate use of social media sites by staff may be the subject of disciplinary action.

COMMENTS POSTED BY PARENTS/CARERS ON SOCIAL MEDIA SITES

Parents/carers will be made aware of their responsibilities regarding their use of social media via this policy (in particular when their child joins the School), the School website, letters and School newsletters:

- Parents should not form online friendships or enter into any online communication with pupils (other than their own children)
- Parents are requested and expected not to post images (photos and videos) of pupils other than their own children on any social media sites, unless they have the express permission of the parents of all other children pictured
- Parents are asked to raise queries, concerns or complaints about the School directly with the School, rather than posting any such comments on social media sites
- Parents should not post malicious, harmful or fictitious comments on social media sites about the School and any member of staff or the wider School community

DEALING WITH INCIDENTS OF ONLINE (CYBER) BULLYING

All cases of online bullying will be dealt with in accordance with the School's Anti-Bullying policy.

The School can take action with reference to any incident that takes place outside school hours if it:

- Could have repercussions for the orderly running of the School;
- Poses a threat to a pupil or member of the School community; and
- Could adversely affect the reputation of the School, or its employees/ governors.

COMMUNICATING THE SCHOOL'S ACCEPTABLE USE POLICY & CODE OF CONDUCT FOR ICT AND SOCIAL MEDIA

Informing Pupils
Pupils are informed that their Internet use is monitored and are given instructions and guidance on the safe and responsible use of the Internet.

Informing Staff
On induction, new staff meet with the Head of IT and the School's AUP Policy is explained, received and read. A hard copy is available in the policies folder in the Staff Room. A soft copy is included within the Resources directory on the network. Staff are regularly reminded of the existence of the policy by the IT support team and in staff meetings. Internet use is monitored and can be traced to an individual user.

Informing Parents/carers
Parents/carers will be made aware of their responsibilities regarding their use of social media via this policy (in particular when their child joins the school), the School website, letters and School newsletters.

SECURITY

The School network is protected by anti-virus software and a firewall. The anti-virus software updates daily. School data is backed up daily. Internet content is monitored by Smoothwall Guardian web filtering software. Network access can be blocked as a sanction.

CODE OF CONDUCT FOR ICT

The Staff Code of Conduct for ICT and Social Media is included as Appendix 1 to this Policy

The Pupil Code of Conduct for ICT and Social Media is included as Appendix 2 to this Policy

The Parent/Carer Code of Conduct for ICT and Social Media is included as Appendix 3 to this Policy

This policy can be made available in large print or other accessible format if required.

Authorised by	
	M Campbell
	Chair of Governance & Compliance Committee
Date 21/11/17	
Approved by	
	M Pyper
	Chair of Governors
Date 21/11/17	
Last Reviewed	November 2016
Next Review	November 2018

APPENDIX 1

STAFF CODE OF CONDUCT FOR ICT AND SOCIAL MEDIA

This document aims to ensure that all members of staff accept and meet their professional responsibilities when using information systems and when communicating with pupils.

- All teaching staff are issued with a laptop computer and these remain the property of the School and must be returned when staff leave employment at the School.

- ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, and social networking sites. ICT use may also include use of personal ICT devices when used for School business.

- School information management systems (WCBS 3Sys) may not be used for private purposes without specific permission from the Headmaster.

- Access to 3Sys via the School network is available to all staff. Staff must ensure this management data is not accessed in a public place. If the computer is left unattended, users must log off or lock the computer.

- The use of School information systems, internet and email may be monitored and recorded to ensure compliance with this Code of Conduct.

- Staff must recognise the need for security of School systems and not disclose any password or security information to anyone other than an authorised system manager.

- The user of a laptop is responsible for all personal files stored on the computer. It is strongly recommended that these files are backed up regularly.

- Personal data, ie of pupils, parents or staff, must at all times be stored securely and used appropriately, whether in School, taken off the School premises or accessed remotely.

- Copyright and intellectual property rights should be respected.

- Any incidents of concern regarding children's safety should be reported to the Designated Safeguarding Lead or Headmaster.

- Electronic communications with pupils must be compatible with the member of staff's professional role. Staff should not store pupils' mobile phone numbers on their personal phones, neither should pupils have access to staff's personal phone numbers.

- Staff should use School cameras when taking photographs for School purposes. Images may not be stored on private computers. Mobile phones must not be used for taking pupil photographs.

- E-safety for pupils in your care should be promoted at all times and will help them to develop a responsible attitude to system use, communications and publishing.

- Staff are expected to store School ICT equipment securely and to take reasonable care against damage when it is used or transported.

- Staff are expected to take responsibility for computer rooms and equipment when accessing them with pupils. Pupils are not allowed to access computer rooms without staff supervision

- Limited use of e-mail and Internet facilities for personal purposes is permitted. The School acknowledges that personal use may occur from time to time. Any such use must be in accordance with this Policy and must not disrupt staff duties. Abuse or excessive use of the e-mail and/or Internet will be dealt with through the disciplinary procedure.

- Staff must set their privacy settings on all personal social media accounts to the highest possible level.

- Staff must not conduct or portray themselves, or allow friends to portray them, in a manner which may:
    - Bring the School into disrepute;
    - Lead to parental complaints;
    - Be considered derogatory towards the School and/or its employees;
    - Be considered derogatory towards pupils, parents or governors
    - Bring into question their appropriateness to work with children

- Staff must not form online friendships or enter into communication with parents via social media sites.

- Staff must not form online friendships or enter into any online communication with pupils.

- Staff must report any communication received from pupils or 'friend requests' on any personal social media sites to the School's designated Safeguarding Lead responsible for child protection.

- Staff must not make any posts or comments that refer to specific, individual matters related to the School and members of its community on any social media accounts.

The School may exercise its right to monitor the use of the School's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the School's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

This code of conduct is designed to protect staff and pupils in line with current safeguarding guidance

APPENDIX 2

PUPIL CODE OF CONDUCT FOR ICT AND SOCIAL MEDIA

- **Never share a password with anyone** – not even your best friend. If you suspect that someone knows it, see the IT Manager (Mr Knight) as soon as possible.
- **Never allow anyone access to your user area** – send files by e-mail to a friend or home as an attachment.
- **Always log off before leaving a computer** –never leave yourself logged in to an unattended computer**.**
- **Keep safe -** Never give a stranger any information about yourself or details of where you live. If you receive any communication you are unsure of ask a member of staff.
- **Use appropriate language** – the e-mail system is monitored.
- **Don't suffer cyber bullying** – report to a teacher and forward any e-mail or other material (text, tweet or facebook post for example) that offends you.
- **Do not be responsible for cyber bullying** – be careful not to post anything online that might cause upset to others or be interpreted as bullying
- **Do not attempt to download or install software** – use only the software provided.
- **Avoid the spreading of computer viruses.**
- **Always give credit for information or pictures obtained from the internet** – observe copyright law.
- **Do not eat or drink close to any computer equipment or peripherals.**
- **The use of the internet at School must only be in support of learning**.
- **Unauthorised use of social networking sites is prohibited whilst at School.**
- **All internet access and activity is monitored by the School.**

APPENDIX 3

PARENT/CARER CODE OF CONDUCT FOR ICT AND SOCIAL MEDIA

This document aims to ensure that parents and carers use social media in a way that safeguards pupils and does not damage the reputation of the School, any member of staff or the wider School community.

- Parents should not form online friendships, or enter into any online communication with pupils (other than their own children).

- Parents should not to post images (photos and videos) of pupils (other than their own children) on any social media sites, unless they have the express permission of the parents of all other children pictured.

- Parents should raise queries, concerns or complaints about the School directly with the School, rather than posting any such comments on social media sites.

- Parents should not post malicious, harmful or fictitious comments on social media sites about the School and any member of staff or the wider School community.