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 E-Safety Policy, 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;
- that staff are protected from potential risk in their use of ICT in their everyday work; and
- 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 users have the right to equal access to resources and children in Year 7 also have access to personal Chromebooks lent to them by school. 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. Users may be asked to remove files if total system storage space becomes low. It is each individual's responsibility to organise their user area or their Chromebooks and to make private files secure.

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts.

All official school business must be conducted on school systems, and it is not permissible to use personal email accounts for school business.

The Right to Privacy in Electronic Communication and Work
Files may be accessed by the IT 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.

Staff, parents and pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

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 Username 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 Username. 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 the IT Support Team or designated teachers. Teachers can change passwords via tools provided by IT 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 Chromebooks or any school equipment, for example through moving or disconnecting mice or keyboards, will involve sanctions such as reimbursement. If equipment is damaged or lost this should be reported to the IT Support Team without delay.

Use of the Network

Users should not knowingly interfere with the performance of the network in any form without consulting the IT Support Team. 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.

In a period of remote learning, it may be necessary for teachers to share copyrighted material with pupils online that they would legally be able to use in the classroom. Under these circumstances teachers are able to share media online provided that the conditions below are met.

Wording to accompany any copyrighted media:

This media has been used under the exemption of Teaching in the Copyright, Designs and Patents Act 1988. The further distribution of this media is prohibited.

Conditions to publishing copyrighted media

- It must be used only when it is necessary and appropriate to be used within a lesson.
- Media must be uploaded to the secure distance learning network if possible.
- It must only appear in an area which is accessible to staff, pupils and parents (not publicly).
- Ensure that media is attributed correctly.
- If using audio, you must not use images of the artist or cover work from albums.
- If using audio, please use a maximum of 30 seconds.
- Only host this media digitally for as long as is required.

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.

Retention of digital data
Staff and pupils must be aware that all emails sent or received on School systems will be routinely deleted after 2 years and email accounts will be closed and the contents deleted within 1 year of that person leaving the School. Important information that is necessary to be kept should be held on the relevant personnel or pupil file, not kept in personal folders, archives or inboxes. Hence it is the responsibility of each account user to ensure that important information is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the School's email deletion protocol.

If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact the IT Manager.

Children's use of mobile devices
Children are not allowed to use personal mobile devices during the day.

In the boarding house

Internet disabled mobile devices are allowed for children in Years 7 and 8 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.

On School trips

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

Breach reporting
The law requires the School to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the School regardless of whether the personal data falls into a third party's hands. This would include:

- loss of a device, USB stick or a physical file containing personal data;
- any external hacking of the School's systems, eg through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax, email, Direct or Instant Message ;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The School must generally report personal data breaches to the ICO without undue delay (ie within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or pupils become aware of a suspected breach, please notify the Finance Director as Privacy Officer.

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 outside of School provided systems 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 School social media sites by staff should be referred to the Headmaster in the first instance and may lead to disciplinary action being taken.

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 e-Safety and Cyberbullying 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 or 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 IT Manager and the School's AUP Policy is explained, received and read. A hard copy is available in the policies folder in the School Office. A digital copy is included within the Staff 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.

<u>SECURITY</u>

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.

<u>CODE OF CONDUCT FOR ICT</u>

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	
	C Kay
	Chair of Governance & Compliance Committee
Date 23rd November 2021	
Approved by	
	M Pyper
	Chair of Governors
Date 23rd November 2021	
Last Reviewed	November 2020
Next Review	November 2022

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, tablet computers, 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 (iSAMS or WCBS PASS) may not be used for private purposes without specific permission from the Headmaster.

- Access to iSAMS 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. While it is the School's clear policy, in order to safeguard both children and staff, not to use personal devices to photograph children, staff are occasionally permitted to use their personal devices if the following guidelines are adhered to.

  Staff should only use a personal device if a school device is not available.

Guidelines/declaration:

- I am aware of children who should not have their photograph taken (a list of photography permissions is held by the Front Office).
- I will never use a personal device to take photographs of children in the Pre-prep.
- I will ensure children are appropriately dressed in any photographs taken.
- I will not take photographs of any children who are not Beaudesert Park School pupils.
- I will transfer any photographs to a school device and **delete** them from my personal device, including from deleted folders, automatic back-ups and cloud storage systems, within 24 hours.

- 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, and seek assistance from the IT Department if they need help with this.

- 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 outside of School provided systems 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

- **All use of school devices and services must only be in support of learning**.
- **Never share a password with anyone** – not even your best friend. If you suspect that someone knows it, see your IT teacher or the IT Support Team 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.**
- **Unauthorised use of social networking sites is prohibited whilst at School.**
- **All internet access and activity is monitored by the School.**
- **Ensure personal devices including Chromebooks are named and all relevant checks with IT support staff are made.**

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 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 not attempt to discover or contact the personal email addresses or social media accounts of staff.

- 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, any member of staff or the wider School community.