Culford

Information Communication Technologies (ICT Policies)

Overview

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. Information and Communications Technology covers a wide range of resources including web-based and mobile learning.

It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. The internet technologies children and young people are using both inside and outside of the classroom are wide-ranging. Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Culford School, we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

The school community captures, processes, stores and shares personal data on pupils, staff, parents and third parties to help them conduct their day-to-day activities. This personal data could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of personal data may result in data breach, which may result in none compliance with current data protection laws. This may also leave the School or a member of the School Community exposed to negative media coverage, and potentially damage the reputation of the School.

Everybody in the school has a shared responsibility to secure any information whether personal and /or special category used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them. Both this policy and the Acceptable Use Policy Agreements are inclusive of both fixed and mobile internet technologies provided by the school, and technologies owned by pupils and staff, but brought onto school premises.

Safety

The Headmaster and Board of Governors have ultimate responsibility to ensure that eSafety policy and practices are embedded and monitored in the school. Culford School has a named eSafety co-ordinator who reports directly to the member of senior leadership team with responsibility for eSafety within each school. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance and brief the school leadership team appropriately.

Culford

This policy, supported by the School's Acceptable Use Policy Agreements for staff and pupils and its Data Protection Policies are designed to protect the interests and safety of the whole school community. It is linked to other school policies including child protection, health and safety, behaviour/ pupil discipline and PSHE.

The School provides opportunities within a range of curriculum areas to teach about eSafety. Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.

Pupils are made aware of the relevant legislation when using the internet. They are taught about copyright and respecting other people on the internet. Pupils are made aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also made aware of where to seek advice or help if they experience problems when using the internet and related technologies. Pupils are taught to critically evaluate materials and learn good searching skills through the curriculum.

Teachers receive regular information and training on eSafety issues. Details of eSafety staff training are available from the member of senior leadership team responsible for staff development.

All new staff receive information on the school's Acceptable Use Policy Agreement as part of their induction. All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community. All teachers are encouraged to incorporate eSafety activities and awareness within their curriculum areas.

Incidents

Some internet activity is illegal and is banned from school and all other ICT systems. Other activities are banned and could lead to criminal prosecution. There are however a range of activities which may be legal but are inappropriate in a school context, either because of the age of the users or the nature of those activities. School policy restricts certain internet usage as follows:

Uploading, downloading, possessing or transmitting material that falls under the following headings, including the attempt to so do:	**Acceptable**	**Unacceptable**	**Illegal**
Child sexual abuse images			X
Illegal acts under child protection, obscenity, computer misuse or fraud legislation			X
Adult material that potentially breaches the Obscene Publications Act			X
Criminally racist material in UK			X

Pornography		X	
Any kind of discrimination		X	
Racial or religious hatred or threatening behaviour			X
Information which may be offensive or bring the bring the school into disrepute		X	
Using school systems to run a private business		X	
Attempting to bypass the filtering or other safeguards employed by Culford		X	
Commercial software or any copyrighted materials without the necessary permissions			X
Revealing or publicising confidential or proprietary information		X	
Creating or propagating computer viruses or other harmful files		X	
High volume network traffic that causes network congestion and hinders work		X	
On-line gaming (educational)	X		
On-line gaming (non-educational) or gambling		X	
On-line shopping / commerce	X		
File sharing (educational)	X		
File sharing (non-educational)		X	
Use of social networking and video broadcasting sites e.g. YouTube, Skype	X		

Responding to Incidents of Misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible use, or deliberate misuse. If any apparent or actual misuse appears to have occurred the protocol below should be followed:

- Save all evidence, do not shutdown or logoff the device, secure and isolate the device.
- If appropriate arrange suspension of the user account with IT Services.
- If the incident involves a member of staff do not approach that member of staff directly.
- If the incident involves a pupil / child record any facts and do not ask any leading questions.
- If the incident is deemed to be a child protection issue contact the Designated Safeguarding Lead.
- If not contact the Head of IT Services or Head of ICT and inform a Deputy Head.
- Ensure a full record has been taken of events.

Email

The use of email is an essential means of communication for both staff and pupils. In the context of Culford School, email should not be considered private. Educationally, email can also offer significant benefits. All users need to understand how to style an email in relation to good network etiquette.

Culford

Managing Email

The School gives all staff and pupils their own email account to use for all school business as a work based tool. This minimises the risk of receiving unsolicited or malicious emails and avoids the risk of personal information being revealed. It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. The school email account must be used for all school business. The school automatically adds a standard disclaimer to all email correspondence, and under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

Pupils may only use school approved accounts on the school system and only for educational purposes. The forwarding of chain letters is not permitted. All pupil email users are expected to adhere to the generally accepted rules of etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission. Pupils must immediately tell a teacher or trusted adult if they receive an offensive email. Staff must inform their line manager.

However you access your school email, all the school email policies apply. The use of internet based webmail except Culford Outlook Web Access services for sending, reading or receiving business related email is not permitted. All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

Sending Emails

If emailing personal, confidential, classified or special category data to external third parties or agencies, refer to the relevant section below.

Use your own school email account so that you are clearly identified as the originator of a message. If you are required to send an email from someone else's account, always use the 'Delegation' or 'send as' facility so that you are identified as the sender. Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate. Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments. An outgoing email greater than five megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming email.

Receiving Emails

Check your email regularly. Activate your 'out-of-office' notification when away for extended periods. Use the 'Delegation' facility within your email software so that your email can be handled by someone else while you are not at work. Never open attachments from an untrusted source; consult IT Services first. Do not use the email systems to store attachments; detach and save business related work to the appropriate drive/folder. The automatic deletion of emails is not allowed.

Culford

Emailing Personal, Special Category, Confidential or Classified Information
Assess whether the information can be transmitted by other secure means before using email; emailing confidential data is not recommended and should be avoided wherever possible. The use of Internet based webmail services for sending email containing special category information is not permitted. Where your conclusion is that email must be used to transmit such data exercise caution when sending the email and always follow these checks before releasing the email:

- Verify the details, including accurate email address, of any intended recipient
- Verify the details of a requestor before responding to email requests for information
- Do not copy or forward the email to any more recipients than is absolutely necessary
- Do not send the information to anybody whose details you have been unable to verify
- Where possible send the information as an encrypted document attached to an email
- Provide the encryption key or password by separate contact; preferably by telephone
- Do not identify such information in the subject line of any email
- Request confirmation of safe receipt.

Internet Access
The internet is an invaluable resource for education, business and social interaction, but also a potential risk to young and vulnerable people. All use of the Culford network for internet usage is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet
Staff will preview any recommended sites before use and if Internet research is set for prep, specific sites will be suggested that have previously been checked by the teacher. All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources and all users must observe copyright of materials from electronic resources.

Users must not post personal, special category, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience; nor reveal names of colleagues, pupils, parents or third parties or any other confidential information acquired through your position at Culford. On-line gambling or gaming is not allowed. It is at the Headmasters' discretion what internet activities are permissible for staff and pupils and how this is disseminated.

School internet access is controlled through a web filtering appliance. Culford School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; The General Data Protection Regulation, the UK Data Protection Bill, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998. Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required. The school does not allow pupils access to internet logs. The school uses management control tools for controlling and monitoring workstations.

If staff or pupils discover an unsuitable site the incident must be reported immediately to a teacher who will then follow eSafety procedures as necessary. It is the responsibility of the school, by delegation to the IT Services, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines. Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility or IT Services to install or maintain virus protection on personal systems.

Pupils and staff are not permitted to download programs on school based technologies without seeking prior permission from IT Services. If there are any issues related to viruses or anti-virus software, IT Services should be informed through Service Desk.

Personal or Special Category Information
Users must ensure that any School information accessed from your own PC or removable media equipment is kept secure and that computers are left locked to prevent unauthorised access. That any personal, special category, confidential and classified information disclosed or shared with others is accurate; that it is not disclosed to any unauthorised person; and that it does not compromise its intended restricted audience.

Users must ensure the security of any personal, special category, confidential and classified information sent or copied to others. They may only download personal data from systems if expressly authorised to do so by their manager and must keep their screen display out of direct view of any third parties when accessing personal, special category, confidential or classified information. Copies of such data must be securely stored and disposed of after use.

All files containing personal, special category, confidential or classified data must be encrypted wherever possible and hard drives from machines no longer in service must be removed and stored securely or wiped clean. All redundant ICT equipment must be returned to IT Services and will be disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Laws.

Safe Use of Images, Video and Sound Recordings
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 school community or public, without first seeking consent and considering the appropriateness.

Culford likes to share our pupils' achievements with the Culford community and beyond through our termly newsletters, press releases, social media, prospectuses and on our website. One of the most enjoyable and effective ways of doing this is by the use of photographs. However, we take very seriously the issue of child safety in connection with the use of images of children in the public domain. Whilst their involvement may be motivating for pupils, and good for the School, we naturally have a duty of care to our pupils and are concerned that we should use photographs with the appropriate consent.

In line with government guidelines, pupils will remain unidentifiable in Culford promotional publications such as our prospectuses. While we tend not to include pupils' full names alongside the images in newsletters and with photographs issued to the media, if the story is about one particular pupil's achievement, for example, it is clearly impossible for the pupil/s to remain anonymous. Parents are sent a letter when their child joins Culford which asks them to complete and return a reply form if they object to the use of images of their children in the public domain.

This consent is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue. Consent may withdraw permission at any time by contacting the school.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record pupils, this includes when on field trips. However with the express permission of the Headmaster, images, video or sound can be taken provided they are transferred immediately and solely to the School's network and deleted from the staff device.

Pupils should not use personal digital equipment to record others, including when on field trips. However, pupils may record images, video or sound of others with the express permission of a member of staff, providing the material is not inappropriate and is not used inappropriately. Pupils must not take, use, share, publish or distribute images, video or sound of others without their permission.

In EYFS staff are required to hand in their mobile phone in the phone basket in the office during working hours. In the event that an employee has an emergency, or is waiting for an important call, they may request permission to use the nursery phone. If staff are witnessed using a mobile phone in the playrooms, toilets, sleep room or kitchen they may be subject to disciplinary action. Staff are not permitted to use any personal recording devices camera, camcorder, iPad or any other device anywhere in the nursery or Pre Prep. Devices for recording observations for Tapestry are provided.

Storage of Images, Video and Sound Recordings

Recordings of children must be stored on the school's network and nowhere else. Rights of access to this material are restricted to staff and pupils as appropriate and material no longer required will be deleted from the network at the earliest opportunity.

The school uses CCTV for security and safety. The only people with access to this are the Head of IT Services, School Caretakers, the ICT Network technicians; and Sports and Tennis Centre Staff who monitor the CCTV cameras attached to and inside that building. Notification of CCTV use is displayed at the front of the school.

The School operates a dedicated live video streaming service from two courts in the tennis dome. These recordings capture pupils and staff in the area during lessons. Access to this service is restricted and access addresses changed monthly. The school does not have any other webcams on

site and additional projects must be managed through the IT Manager. Misuse of webcams by any member of the school community will result in sanctions.

Conferencing
Skype and other similar services can be used by pupils outside the normal working day to contact parents and guardians. Skype and other similar services should not be used during the working day by pupils and should be turned off. Skype and other similar services should not be used as an instant messaging application. Pupils should not make contact with or accept approaches from unknown individuals or organisations. Skype and other similar services usernames must be marked as private and not included in the global search.

School ICT Equipment
Users are responsible for any activity undertaken on school ICT equipment provided to them. Culford School keeps a record of ICT equipment issued to staff. All ICT equipment must be kept physically secure. Users must save data on a frequent basis. Individuals are responsible for the backup and restoration of any data that is not held on the school's network drive. Personal or special category data should not be stored on the local drives of laptops or desktop PCs or in the shared drive of the schools IT system. Individuals are responsible for any information accessed from their own equipment and must ensure it is kept secure, and that no personal, special category, confidential or classified information is disclosed to any unauthorised person.

Visitors must not plug their hardware into school network points but must be directed to IT Services if network access is required. Unauthorised access or modifications to computer equipment, programs, files or data is an offence under the Computer Misuse Act 1990. On termination of employment all ICT equipment must be returned to IT Services.

Portable & Mobile ICT Equipment
All activities carried out on School systems and hardware will be monitored in accordance with the general policy for school ICT equipment. School data must be stored on the school's network, and not kept solely on mobile equipment. Personal data should be encrypted where possible and the devices have password protection enabled and used. Equipment must be kept physically secure. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey. Devices should not be left in vehicles unattended overnight or for long periods of time. Never leave the device in view and make sure the vehicle is secure. Staff must never use a hand-held mobile phone whilst driving a vehicle.

Users should synchronise all locally stored data with the central school network server on a frequent basis. Portable and mobile equipment must be made available as necessary for anti-virus updates and software installations, patches or upgrades and the installation of any applications or software must only be authorised, fully licensed and installed by IT Services. Portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight. It must be transported in its protective case if supplied.

Culford

Users must report the loss of any school mobile device to the Head of IT Services immediately because the school remains responsible for all costs until the mobile device is reported lost or stolen. School SIM cards must only be used in school provided mobile phones unless authorized by the Head of IT Services. Staff may have to reimburse Culford School for the cost of any personal use of equipment.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning. Mobile devices often offer internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Culford School will manage the use of these devices so that users exploit them appropriately.

The school allows staff to bring in personal mobile phones and devices for their own use.

Pupils are allowed to bring personal mobile devices to the Senior School but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent. Prep and Pre-Prep pupils must leave their personal mobile devices in the designated areas in Cadogan House or the School office. Pupils' personal mobile devices may be used for educational purposes, when authorized by the member of staff responsible. The device user must always ask the prior permission of the bill payer.

The school is not responsible for the loss, damage or theft of any personal mobile device.

The sending of inappropriate digital messages between any members of the school community is not allowed and permission must be sought before any image, video or sound recordings are made on these devices of any member of the school community.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Managing Social Networking

Social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However there are issues regarding the appropriateness of some content, contact, culture and commercialism. Users must think carefully about the way that information can be added and removed by all users, including themselves, from these sites. At present, the school endeavours to deny access to social networking sites to pupils within school during the working day.

Users must be cautious about the information given by others on sites, for example users not being who they say they are. Users should not place images of themselves on such sites owing to the difficulty of removal once online. Users must avoid giving out personal details which may identify

them or where they are. Users must always set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals. Users must be wary about publishing specific and detailed private thoughts online. Users must report any incidents of online bullying to the school.

Staff may only create or use social networking tools to communicate with pupils using a Culford approved platform or other system approved by the Headmaster and made known to the IT Manager.

Telephone Services

School telephones are available in term time for all School business, but only for local or UK calls. Anyone requiring calls outside the UK must see the Head of IT Services. The school has two mobile phones which are usable in Europe. They are available from the School Office for use on school trips. Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases.

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the School, and devices owned by pupils that have been used to access the Culford school network, at any time without prior notice. Authorised ICT staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or pupils without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under Data Protection Laws, or to prevent or detect crime.

Authorised ICT staff may, without prior notice, access the email or voicemail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by authorised staff and comply with Data Protection Laws, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000. Personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted or recorded.

Breaches

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of ICT hardware, software or services from the offending individual. Any breach is grounds for disciplinary action. Breaches may also lead to criminal or civil proceedings.

Any security breaches or attempts, lost or stolen equipment or data, unauthorised use or suspected misuse of ICT, virus notifications, unsolicited emails, and all other policy non-compliance must be

immediately reported to the school's IT Manager or Compliance Officer.

Computer Viruses
All files downloaded from the Internet or received via email will be automatically checked for viruses. However, files on removable media must be checked for any viruses using school provided anti-virus software before using them. Users must never interfere with any anti-virus software installed on school equipment. In the case of a suspected virus, users must stop using the equipment and contact IT Services immediately. The IT Services department will be responsible for advising users of what actions to take.

Data Protection and Security
All staff must follow the School's policies and procedures in relation to the management of personal data which have been written in line with current data protection laws. A large amount of pupil, parent, employee and third party data is held on electronic systems such as the school server, various cloud base systems apps or personal laptops, mobile phones and USB's.

Under General Data Protection Regulations, individuals have the right to request access to the information the school holds about them, Subject Access Request (SAR). This request must be responded to no long than one month after the request was made. It is important that staff understand how to recognise a Subject Access Request and the school polices on responding to it. All SAR's must go through the Compliance Officer.

Full Data Protection Polices can be found in Moodle/Support/Data Protection. The Schools Data Protection Lead is the Compliance Officer who is available for support or to answer any queries you may have about data protection.

New Software or Apps
All new software or apps for school use must be made know to the IT Manager before purchase has taken place. This is to comply with data protection laws. The IT Manager will liaise with the Schools' Data Protection Lead to ensure any data impact assessments, data sharing agreements and data mapping has been carried out before the final purchase of the system.

Security
The School gives relevant staff access to its Management Information System, with a unique ID and password. It is the responsibility of users to keep passwords secure. Staff must be aware of their responsibility when accessing school data. Staff have access to relevant guidance within the Culford ICT Policy, including the Acceptable Use Policy Agreement. Staff must keep all school related data secure, especially all personal, special category, confidential or classified data.

Anyone expecting or sending a confidential or special category fax, should use the Safe Haven Fax procedure:

- Ensure the recipient knows the fax is being sent and that it will be collected at the other end.
- Send the front sheet through first and check that it has been received by the correct recipient.
- Add the rest of the document to the fax and press the redial button.
- Don't leave while transmitting; wait for the original to process and remove it from the fax machine.
- Wait for confirmation of successful transmission.
- Confirm whether it is appropriate to fax to another colleague if they are not there to receive it.
- Use only the minimum information and anonymise where possible.

Passwords

Staff and pupils must always use their own personal passwords to access computer based services and enter them each time they logon. Passwords should not be saved in any automated logon procedures. Staff and pupils should change temporary passwords at first logon and change passwords whenever there is any indication of possible system or password compromise. Passwords should not be recorded on paper or in an unprotected file. Personal passwords should only be disclosed to authorised ICT support staff when necessary, and never to anyone else. All personal passwords that have been disclosed should be changed once the requirement is finished. Passwords should contain a minimum of six characters and be difficult to guess. Staff and pupils who think their password may have been compromised or someone else has become aware of it should report this to IT Services.

User ID and passwords for staff and pupils who have left the school are removed within 24 hours.

Password security is essential for staff. Staff must have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others. Staff must be aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and the Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual users must also make sure that workstations are not left unattended and are locked. Due consideration should be given when logging into the Learning Platform to the browser/cache options for a shared or private computer.

All staff and pupils are expected to comply with password policies at all times

Remote Access

Individual users are responsible for all activity via any of the Culford School remote access facilities. Only equipment with an appropriate level of security for remote access should be used; not, for example, equipment provided in a publically used internet café. To prevent unauthorised access to School systems, users must keep all information such as logon IDs and passwords confidential and not disclose them to anyone. They should avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.

Staff and pupils must protect School information and data at all times, including any printed material produced while using the remote access facility. Particular care must be taken when access is from a non-School environment.

Inventions, Patents, Copyright

You are required to inform the school immediately of any invention, improvement, discovery, process, design or copyright which you create or obtain whilst in the school's employ or as a consequence of it. This will become the absolute property of the school except as otherwise stated by statute. When you leave the school you will return all databases and other information held by you whether developed or maintained by you during the course of your employment with the school.

Communications with the Media

Any member of staff approached by the media should contact the Headmaster's Office as soon as possible or, in his absence a member of the Executive.

Staff should not pass comment to any form of medium on any matter without prior express approval. All responses and comments to the Press are to be approved by the Headmaster, or, in his absence, by the Executive. All communication with the media should be carried out in a courteous and professional manner and calls and emails from the media should be returned promptly by those authorised to do so.

All press releases and Social Media are co-ordinated by the Marketing department. If colleagues wish to promote an event, achievement or activity they should contact the Marketing Department who will be pleased to advise and assist.

All representatives of the media visiting Culford should be accompanied by a member of staff at all times. Press photographers and news broadcasters do not have a right to take pictures or film anywhere on school grounds as it is private property. Any member of staff who sees anyone taking photographs or filming without a school chaperone should report this to reception and to the Marketing Department immediately.

Any member of staff approached by an individual or an organisation seeking information held by the school about themselves or any other person must pass that request, and the reason, to the Headmaster's Office. Staff should not pass comment on individual or release any information without prior express approval from the Headmaster.

Social Media

The creation and moderation of all Culford's social media channels is done by the Marketing Department. This includes forums, discussion groups and blogs as well as the mainstream social channels such as Facebook, Twitter, YouTube, Pinterest, Flickr, Snapchat, Instagram, LinkedIn etc.

We are keen for staff to engage with the school's social Media Activities, but they must only do so through the Marketing Department who will ensure messaging is effectively deployed on the correct platforms.

In addition to this staff may not engage with the School's Social Media as identifiable representatives of Culford. This means that you must not:

- Post comments or other content as an official representative of Culford.
- Respond to positive or negative comments regarding the school. Should you come across comments or other postings that are of interest or concern, you should forward them to the Marketing Department who will handle matters.
- Make references to you being a member of Culford's staff while on Social Media. This includes things such as Social Media biographies and the use of 'Culford' in the naming of any blog, forum or instant messaging accounts. Making reference to your position is permitted on professional networking sites such as LinkedIn.
- Post official Culford footage, images or other media, particularly when children can be seen, on any Social Media Platform.
- Tag any Culford pupil on Social Media. Tagging increases an images profile in internet searches and makes identification possible.
- You must not accept or solicit friendship or follow requests from current pupils or engage with them directly on Social Media. If asked to engage with alumni (former pupils) on social media you should ensure that the Foundation and Marketing Department are aware, to protect your own position.

Other Digital Communications

Employees must refrain from engaging in unsolicited digital dialogue with unknown third parties via email, instant messaging or text. Despite everyone's best efforts unsolicited communications do come through and you should delete or ignore these. If you are in doubt about the genuine nature of any digital communication that you receive to your school email address, please refer to the Head of IT Services. Should a request come through from a journalist from any medium you must forward it to the Headmaster's Office.

Breach of the Social Media Policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach. Any employee suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and log in details so far as this is consistent with the right of an individual to private and family life.

Employees may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request in itself may result in disciplinary action.