ACCEPTABLE USE OF ICT POLICY

Oswestry School
Founded 1407

1. Contents

2. Introduction

2.1. Oswestry School prides itself on its innovative approach to the use of ICT. We are progressive in our approach and wholeheartedly encourage the sensible use of technology in all the teaching and administrative functions of the school.

2.2. This policy encompasses the following technologies, but it is not limited to them:

2.2.1. Websites
2.2.2. E-mail, instant messaging and chat rooms
2.2.3. Social media, including Facebook, Twitter, Snapchat, Instagram etc.

2.2.4. Mobile/ smart phones with text, video and/or web functionality
2.2.5. Other mobile devices with web functionality
2.2.6. Gaming, especially online
2.2.7. Learning platforms and virtual learning environments
2.2.8. Blogs and wikis
2.2.9. Podcasting
2.2.10. Video broadcasting
2.2.11. Music downloading

2.3. This policy relates to all staff, governors, visitors and pupils. It is inclusive of both fixed and mobile internet technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc). It includes technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

2.4. This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: safeguarding and behaviour (including the anti-bullying) policy and our PSHEE scheme of work. Reference is also made to the school's legal obligations such as they fall under 'Prevent Duty'.

3. Data Security

3.1. Oswestry School recognises that it holds potentially sensitive personal data on pupils and staff. The school has in recent years embraced cloud computing, the school's central database is on the iSAMS database in the cloud. The single central register is stored in a locked-down Google sheet. Staff and pupils are permitted to use their own devices in school and are periodically reminded of the importance of security and good data management. Specifically staff and pupils are encouraged to:

3.1.1. Lock down their devices when they are not in front of them

3.1.2. Password protect their devices

3.1.3. Use two-factor authentication, where doing so is practical

4. Monitoring

4.1. Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice.

4.2. Authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving members of the school community, 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 the Data Protection Act 1998, or to prevent or detect crime.

4.3. Authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any school related issues retained on that account.

4.4. All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

4.5. Note that personal communications using school ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

5. E-mail

5.1. The use of e-mail within Oswestry School is an essential means of communication for all members of the community. E-mail should not be considered private. The school recognises that educationally, e-mail offers significant benefits including facilitating direct written contact between pupils and staff working on different projects. The school also recognises that pupils need to understand how to operate e-mail and compose messages appropriately as part of their preparation for life beyond school.

6. Managing e-Mail

6.1. Oswestry gives all staff and pupils their own e-mail account to use for all school business. This is to protect members of the school community and minimise the risk of receiving unsolicited or malicious e-mails. It also avoids the need for personal contact information to be revealed.

6.2. 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 e-mail histories can be traced.

6.3. Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses. The school email account should be the account that is used for all school business.

6.4. The school requires a standard disclaimer to be attached to the base of all e-mail correspondence. E-mails from staff should also have the latest school-endorsed signature block attached to them. This process is automated.

6.5. All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper. Staff are encouraged to use iSAMS as a means to send e-mail communications to parents. E-mails from iSAMS are school branded and will be sent to the correct contact addresses as stored in the school's central data

repository.

6.6. Staff sending e-mails to external organisations, parents or pupils are advised to cc their line manager.

6.7. School e-mail accounts are intended for the use of the account holder only. Under no circumstances should account details be shared; nor should e-mails be sent from an e-mail address by anyone other than the address owner. Sending an e-mail from someone else's account - with or without their permission - is a serious offence.

6.8. Pupils may only use school approved e-mail accounts for sending e-mails that are to do with the day-to-day school business. Staff should not engage in email conversations from a pupil who uses a non-school address.

6.9. E-mails created or received as part of your work in school will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:

6.9.1. Delete all e-mails of short-term value

6.9.2. Carry out frequent housekeeping on all folders and archives

6.9.3. Note that the forwarding of chain letters is not permitted in school

6.10. All e-mail 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 e-mail communication, or arrange to meet anyone without specific permission.

6.11. Pupils must immediately tell a teacher or trusted adult if they receive an offensive e-mail. Staff must inform their line manager if they receive an offensive e-mail.

6.12. Pupils are introduced to e-mail as part of the ICT/Computing scheme of work and as part of the induction process laid on by form tutors at the start of a new year, or on the arrival of a new pupil.

6.13. Wherever members of the school community access their school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

7. Sending e-Mails

7.1. If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section e-mailing Personal, Sensitive, Confidential or Classified Information.

7.2. Use your own school e-mail account so that you are clearly identified as the originator of a message.

7.3. Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.

7.4. Do not send or forward attachments unnecessarily. Whenever possible send documents in Google format. Share them appropriately to save having to make multiple copies and to ensure a contemporary copy is used.

7.5. School e-mail is not to be used for personal advertising.

8. Receiving E-mails

8.1. Check your e-mail regularly.

8.2. Activate your 'out-of-office' notification when away for extended periods.

8.3. Never open attachments from an untrusted source.

8.4. Do not use the e-mail system to store attachments. Detach and save business related work to the appropriate shared drive or folder.

8.5. The automatic forwarding and deletion of e-mails outside the domain is not allowed.

9. E-mailing Personal, Sensitive, Confidential or Classified Information

9.1. Where your conclusion is that e-mail must be used to transmit such data obtain express consent from your line manager to provide the information by e-mail.

9.2. Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

9.2.1. Verify the details, including accurate e-mail address, of any intended recipient of the information

9.2.2. Verify (by phoning) the details of a requestor before responding to e-mail requests for information

9.3. Do not copy or forward the e-mail to any more recipients than is absolutely necessary.

9.4. Do not send the information to any body/person whose details you have been unable to separately verify (usually by phone).

9.5. Do not identify such information in the subject line of any e-mail.

9.6. Do request confirmation of safe receipt.

10. Social Media

10.1. A social networking site is any website which enables its users to create profiles, form relationships and share information with other users. It also includes sites which have online discussion forums, chat-rooms, media posting sites, blogs and any other social

space online. It includes but is not limited to, sites such as Facebook, Bebo, Ping, Twitter, Instagram etc.

10.2. This policy applies to the use of social media for both business and personal purposes, whether during working hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff or pupils or any other IT equipment.

10.3. Staff breach of this 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 member of staff 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 login details so far as this is consistent with the right of an individual to private and family life.

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

11. Relationship with other School policies

11.1. If an internet post would breach any of our policies in another forum it will also breach them in an online forum. For example, staff are prohibited from using social media to:

11.1.1. breach our obligations with respect to the rules of relevant regulatory bodies;
11.1.2. breach any obligations they may have relating to confidentiality;
11.1.3. breach our disciplinary rules;
11.1.4. defame or disparage the School or our affiliates, parents, staff, pupils, business partners, suppliers, vendors or other stakeholders;
11.1.5. harass or bully other staff in any way or breach our Anti-bullying policy;
11.1.6. unlawfully discriminate against other staff or third parties or breach our Equal Opportunities policy;
11.1.7. breach our Data Protection policy (for example, never disclose personal information about a colleague, pupil or parent online);
11.1.8. breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).

11.2. Behaviour online can be permanent and so staff and pupils must be extra cautious about what they say as it can be harder to retract.

11.3. Staff and pupils must also be aware of the particular risks to internet security that social media presents and so to comply with this policy on internet security extra measures necessary extra measures must be taken so as to not allow any of their actions on social media sites to create vulnerability to any School systems.

11.4. Staff who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

12. Staff responsible use of social media

12.1. Staff must be aware that their role comes with particular responsibilities and they must adhere to the School's strict approach to social media.

12.2. Staff must:

12.2.1. ensure that wherever possible their privacy settings on social media sites are set so that pupils cannot access information relating to their personal lives;
12.2.2. seek the blessing of the headmaster for posting on open forums where they do so in their capacity as a school employee
12.2.3. never post material in such a forum that might bring the school into disrepute, or otherwise harm its interests
12.2.4. report to their Head of Faculty or Line Manager immediately if they see any information on the internet or on social networking sites that disparages or reflects poorly on the School;
12.2.5. immediately remove any internet postings which are deemed by the School to constitute a breach of this or any other School policy;
12.2.6. consider whether a particular posting puts their effectiveness as a staff member at risk;
12.2.7. post only what they would be happy for the world to see, even in forums that are ostensibly private

12.3. Staff must not:

12.3.1. provide references for other individuals, on social or professional networking sites, as such references whether positive or negative can be attributed to the school and create legal liability for both the author of the reference and the school;
12.3.2. post or publish on the internet or on any social networking site, any material that allows for the identification of colleagues, parents or pupils;
12.3.3. use commentary deemed to be defamatory, obscene, proprietary, or libellous. Staff must exercise caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterisations;
12.3.4. discuss pupils or colleagues or publicly criticise the School or staff;
12.3.5. post images that include pupils on private social media channels;
12.3.6. initiate friendships with pupils on any personal social network sites;
12.3.7. accept pupils as friends on any such sites; staff must decline any pupil-initiated friend requests;
12.3.8. use open-forum social networking sites as part of the educational process e.g. as a way of reminding pupils about essay titles and deadlines.

13. Personal use of social media

13.1. We recognise that staff may work long hours and occasionally may desire to use social media for personal activities at the office or by means of our computers, networks and other IT resources and communications systems. Such occasional use is authorised, so long as it does not involve unprofessional or inappropriate content and does not interfere with employment responsibilities or productivity.

13.2. Indeed, the constructive use of social media, as a means of connecting with other professionals, as a means of learning, and as a means of advancing the interests of the School is positively encouraged. See this article, written by one of our deputy heads, as an illustration of what we mean by this.

13.3. While using social media at work, circulating chain letters or other spam is never permitted. Circulating or posting commercial, personal, religious or political solicitations, or promotion of outside organisations unrelated to the organisation's business are also prohibited. Staff must ensure that their use of social media does not create any breaches of internet security and therefore must be careful to avoid any applications that might interrupt our IT systems. Excessive use of social media that interrupts staff productivity will be subject to a disciplinary procedure, consistent with this policy.

14. The monitoring of social media

14.1. The contents of our IT resources and communications systems are our property. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

14.2. We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

14.3. We may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

14.4. Do not use our IT resources and communications systems for any matter that you wish to be kept private or confidential from the organisation.

15. Social media and the end of employment

15.1. If a member of staff's employment with our School should end, for whatever reason, any personal profiles on social networking sites should be immediately amended to reflect the fact that you are no longer employed or associated with our School.

15.2. All professional contacts that a member of staff has made through their course of employment with us belong to our School, regardless of whether or not the member of staff has made social media connections with them.

16. Communicating with Students

16.1. Following the implementation of a new offence in April 2017 under section 67 of the Serious Crime Act 2015 criminalising anyone over the age of 18 who intentionally communicates sexually with a child under the age of 16 or with an intention to encourage a child to make a communication which is sexual, the School reiterates that all staff must abide by all communication procedures within the school including this policy. This offence applies equally to online and offline communications irrespective of the way the communication is made (for example it will apply to oral communications and written notes as well as to e-mails and text messages).

17. eSafety

17.1. 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 and that some have minimum age requirements, **usually 13 years.**

17.2. Staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues. **Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children.**

18. eSafety in the Curriculum

18.1. ICT and online resources are increasingly used across the curriculum. At Oswestry believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

18.2. The school teaches internet skills in Computing/ICT/PSHEE lessons (schemes of work are available on request)

18.3. The school provides opportunities within a range of curriculum areas to teach about eSafety. eSafety forms an integral part of the 1-3rd form ICT programme.

18.4. Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the eSafety curriculum.

18.5. Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities.

18.6. Pupils are aware of the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying. Cyberbullying is broached through the school's PSHEE and mentoring programme at least once a year. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, anti-bullying ambassadors, Childline or the CEOP report abuse button.

18.7. Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

19. eSafety Skills Development for Staff

19.1. Our staff receive regular information and training on eSafety

19.2. New staff receive information on the school's acceptable use policy as part of their induction

19.3. All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety

19.4. All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

19.5. The school has a designated e-Safety officer to oversee all matters to do with e-Safety

20. Managing the School eSafety Messages

20.1. We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used

20.2. The eSafety message is introduced to the pupils at the start of each school year and periodically throughout

20.3. eSafety posters are prominently displayed around the school site

21. Incident Reporting

21.1. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to a teacher (if you are a pupil) or a your to the ICT department (if you are a teacher). Similarly, all security breaches, lost/stolen equipment or data virus notifications, unsolicited emails, misuse or

unauthorised use of ICT and all other policy non-compliance must be reported.

22. Complaints

22.1. Complaints and/or issues relating to eSafety should be made to according to the how to complain document posted in form rooms or direct to an member of SMT (if you are a teacher).

23. Inappropriate Material

23.1. All members of the school community are made aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to a teacher or line manager, as appropriate.

23.2. Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Helpdesk, depending on the seriousness of the offence; investigation by the Headmaster (or an appointed deputy), immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

23.3. Inappropriate material includes, but is not restricted to: material that encourages discrimination, material that glorifies violence, material that is illegal, material that encourages substance abuse, self-harm or suicide, material the promotes hacking or computer misuse, material that promotes extremism and material that is pornographic.

23.4. Users are made aware of sanctions relating to the misuse or misconduct. All users of the School's computers and WiFi network must agree to terms and conditions making these proscriptions clear.

24. Internet Use

24.1. You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience

24.2. Do not reveal names of colleagues, customers or pupils, others or any other confidential information acquired through your job on any social networking site or blog or other online application.

24.3. On-line gambling is not allowed. Gaming is only allowed at certain times of the day.

24.4. It is at the Headmaster's discretion as to what internet activities are permissible for staff and pupils.

24.5. All staff sign the ICT Code of Practice when they join the school, and are be made aware of any amendments to the policy.

24.6. The school reserves an absolute right to monitor the internet activity of all users on the network. The school also filters internet activity as detailed here.

25. Pupils' use of internet

25.1. Use of the internet, including e-mail, is permitted as directed by the teacher for purposes of research and learning directly related to the curriculum. Outside normal school hours pupils are permitted to use the school's internet and their school e-mail account for personal purposes providing that, in doing so, they do not contravene the rules and expectations laid down elsewhere in this document.

25.2. The school's internet connection is a fast 100Mbs^{-1} connection. However, the bandwidth is not infinite. All users are expected to share the resource. Any use which leads to data transfer of more than 30GB in any monthly period is deemed excessive and could result in the user's account being 'throttled' - the download speed restricted.[1]

25.3. The use of game-style activities should be monitored by the teacher (or member of staff in charge of ICT) to determine suitability. Games which are not age appropriate, contain violence, inappropriate language or behaviour demeaning to others are NOT permitted. Pupils are to follow any directions relating to gaming activity from the supervising member of staff.

25.4. Accessing websites that contain content and images which are not age appropriate, i.e. from a film, television programme or game deemed to be for older viewers is not permitted. This is at the discretion of the supervising member of staff.

25.5. Images from the internet are not to be accessed, downloaded or printed without prior permission from a supervising member of staff.

25.6. Pupils are permitted to view videos through YouTube – many are extremely useful for learning. However, the school reserves the right to withdraw this privilege from individuals or groups if it is felt that it is being misused.

25.7. Personal e-mail, social networking (Facebook, Twitter etc) or instant messaging sites (WhatsApp, Snapchat etc) are NOT to be accessed by pupils during school hours. There are no exceptions to this, even if the pupil is over the age required to sign up for the website. If a member of staff has concerns regarding access to age restricted activities (i.e. a pupil has a Facebook account and is below the age of 13) action may be taken to report pupil activity to the website provider.

25.8. Children should report any misuse of the internet to their teacher.

25.9. Children should be made aware of the possibility and consequences of online bullying.

25.10. When e-mail is required as part of a curriculum based lesson, ALL e-mails transmitted and received will be approved by teaching staff.

25.11. No emails will be approved where they may include information that may offend others

[1] For easy-to-understand guidelines on how much bandwidth typical internet activities use see here. For those who would like to monitor their usage the IT Department recommends: Windows; Mac OS X; iOS; Android.

or where they do not respect the rights, beliefs and feelings of others. Pupils of Oswestry School should always remember that they are representing themselves and our school.

26. Pupil use of the school network

26.1. All pupils will be given a username to access the network. Pupils must log onto the school network using their personal username only.

26.2. ICT code of conduct for pupils

26.3. ICT sanctions

27. Staff use of internet

27.1. Use of the internet on school premises should principally be for school use, e.g. accessing learning resources, educational websites, researching curriculum topics, use of email on school business.

27.2. Use of the school's internet for personal financial gain (including the use of online auction sites), gambling, political purposes or advertising is excluded.

27.3. The school recognises that information can now be accessed online through the 'streaming' of data, i.e. radio, television, music, etc. Teachers and administration staff should only be accessing streamed information if it is of educational interest to a lesson or to its planning. For example, using BBC iPlayer is acceptable if it is the interest of the class and related lessons. Streaming music for personal use is discouraged. This is due to the streaming process placing demands on the school's internet bandwidth; as a result the internet can become slow for all users.

27.4. Teachers should not be accessing the internet for personal reasons whilst teaching children.

27.5. Use of the internet to access any illegal sites or inappropriate material is a disciplinary offence. If accessed accidentally users should report incident immediately to the Head Teacher or Head of ICT where it will be logged.

27.6. Staff must not access any school computer to access social networking sites, such as Facebook, Twitter, etc, for recreational use during normal working hours. Any damage caused to school computer equipment due to accessing these sites is the responsibility of the member of staff, unless authorised by the Headmaster.

27.7. The school recognises that many staff will actively use Facebook, Twitter, and other such social networking sites, blogging and messaging services. Staff must not post material (including text or images) which damages the reputation of the school or which causes concern about their suitability to work with children. Staff must recognise that it is not appropriate to discuss issues relating to children or other members of staff via these networks. Those who post material which could be considered as inappropriate could

render themselves vulnerable to criticism or allegations of misconduct.

27.8. It is never acceptable to accept a 'friendship request' from pupils at the school. It is also extremely inadvisable to accept as friends ex-pupils who are still minors. If a parent of a pupil seeks to establish contact, the member of staff should exercise their professional judgement at all times. The only exception to this is if a member of the same family attends Oswestry School.

27.9. All sensitive data, such as children's details and report comments, should be stored on an encrypted storage device or password protected laptop. Other data, such as lesson plans and resources, may be stored on unencrypted devices.

27.10. Under no circumstances should staff contact pupils, parents or conduct any school business using their personal email addresses.

27.11. ICT code of conduct for staff

28. Use of mobile phones and recording devices

28.1. Whilst it is recognised that members of staff may need to use their own telephone to contact each other, or relay information regarding expected arrival times from trips etc., staff are advised that contact with parents should, wherever possible, be undertaken through the school telephone system. Parents should be discouraged from contacting members of staff on their personal mobile phones. All calls to staff regarding school business should where possible be directed through the main school telephone number. Houseparents have school mobile phones, as do all members of the SMT.

28.2. For the purpose of a School trip, staff may find it expedient at times to use their own mobile phone. Any pupil telephone numbers recorded in a personal device for the purpose of a School trip **must be deleted within 72 hours** of the end of the trip. School mobile phones are available for off-site trips; this avoids the need for staff to give out their personal mobile phone number to pupils on the trip and/or to parents.

28.3. Any photographs of activities including children taken on a personal device must not be shared and should be deleted or transferred to the school network as soon as possible and within 72 hours of the activity ending or the end of the trip (whichever is sooner).

28.4. Mobile phones and other cameras **must never** be used in an area where pupils or staff might change.

28.5. Mobile phones should not be used when teaching, unless in an emergency.

28.6. Sometimes teachers may want to encourage pupils to use their mobile devices for teaching purposes. This is fine, providing their use is tightly controlled and recordings - still, video or audio - pass into the ownership of the teacher at the end of the exercise.

28.7. Pupil use of mobile phones is governed by mobile phones and electronic devices policy.

29. Use of digital images

29.1. Any photos or videos taken by teachers, other adults (including parents), and the children themselves during ANY school activity (including educational visits) should not be put on public display or published anywhere on the internet (including social networking websites).

29.2. The above excludes the publication of photos on the Oswestry School website and social media accounts, within the school magazine, for the purpose of school related publicity, and where used by the school for educational / display uses.

29.3. Further, more detailed, information on taking, storing and using of images at Oswestry is in a separate policy document.

30. **Use of school hardware** (laptops, cameras, recording equipment, etc.)

30.1. Use of school laptops, cameras, video cameras and recording equipment is limited to activities directly related to school activity. They can be used during lessons, sporting activities, school visits and residential trips. They are not for personal use.

30.2. All data must be transferred to the school network as soon as possible to ensure that data is saved and protected. Once copied to the network the data must be deleted from the recording equipment.

30.3. If travelling with these hardware items, and they contain information relating to staff or pupils, i.e. address details, photographs or reports, ensure that files are encrypted and password protected.

30.4. All members of staff will be given a username and password. Staff must log onto the school network using their personal username and password only. Staff must not access the school network using the administrator username and password unless given permission

30.5. Staff must not download software onto the school network before first liaising with the Helpdesk to check for suitability. Software that is installed and is deemed not necessary for use in the school context will be deleted.

31. Annual Check Matrix:

Policy:	Acceptable use of ICT Policy
Applies to:	All staff and pupils in both the senior and junior schools
Original:	https://goo.gl/Oi007Z
Author(s):	Sue Nancini/Tim Jefferis

Approved by:	Tim Moore-Bridger (Governor) Feb 2014; Michael Symonds (Governor) 26/1/15; JPN (Feb 2015)
Annual Review:	*I certify that I have reviewed this policy, and verify that, to the best of my knowledge, it reflects current legislation and is in accordance with the wishes of the Governing Body and Headmaster.*
Reviewer to enter initials next to appropriate date:	TJJ May 13; TJJ Mar 14; SAN June 14; TJJ Nov 14, PAB Jan 15, JPN Feb 15; JPN Nov 15; JPN 4/2/16; TJJ 5/1/2016; JPN 7/1/2017