ACCEPTABLE USE OF IT POLICY

Oswestry School
Founded 1407

CONTENTS

ANNUAL CHECK MATRIX

Policy:	Acceptable use of IT Policy
Applies to:	All staff and pupils in both the senior and junior schools including EYFS
Source:	ISBA policy (IT: Acceptable Use Policy for Schools October '23)
Author(s):	Sue Nancini/Tim Jefferis. Updated by PA Bowd (Bursar) 3/1/19, 12/8/19
Approved by:	Tim Moore-Bridger (Governor) Feb 2014; Michael Symonds (Governor) 26/1/15, Jonathan Wastling (Governor) 4/3/21
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, SAN 15/01/18 [awaiting post-GDPR review by IT advisers] JPN 17/10/18; JPN 14/1/19, PAB 13/10/20, 25/1/22, JH(DSL) 16/5/23, AEA 14/09/23, PAB 18/12/23

Oswestry School
Founded 1407

1. SCOPE OF THIS POLICY

1.1. This policy applies to all members of the school community (staff or pupils) who use school IT systems, as a condition of access. Access to school systems is not intended to confer any status of employment on any contractors.

2. ONLINE BEHAVIOUR

2.1. Refer to Online Safety policy.

2.2. As a member of the school community you should follow these principles in all of your online activities:

2.2.1. The school cannot guarantee the confidentiality of content created, shared and exchanged via school systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.

2.2.2. Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).

2.2.3. Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.

2.2.4. Do not access or share material that infringes copyright, and do not claim the work of others as your own.

2.2.5. Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.

2.2.6. Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

3. USING THE SCHOOL'S IT SYSTEMS

3.1. Refer to BYOD policy.

3.2. Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

3.2.1. Only access school IT systems using your own username and password. Do not share your username or password with anyone else.

3.2.2. Do not attempt to circumvent the content filters or other security measures installed on the School's IT systems, and do not attempt to access parts of the system that you do not have permission to access.

3.2.3. Do not bring into School inappropriate material that you have previously downloaded onto a device.

3.2.4. Do not attempt to install software on, or otherwise alter, school IT systems.

3.2.5. Do not use the School's IT systems in a way that breaches the principles of online behaviour set out above.

3.2.6. Remember that the School monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.

4. PASSWORDS

4.1. Refer to Online Safety policy (5.4).

4.2. Passwords protect the School's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

5. USE OF PROPERTY

5.1. Any property belonging to the School should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the IT Helpdesk.

6. USE OF SCHOOL SYSTEMS

6.1. 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. Again, please be aware of the school's right to monitor and access web history and email use.

7. USE OF PERSONAL DEVICES OR ACCOUNTS AND WORKING REMOTELY

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

7.2. Personal devices must be subject to appropriate safeguards in line with the School's policies, including two-factor authentication, encryption and use of a security system to access the personal device, in accordance with our BYOD policy.

7.3. Mobile phones should not be used when teaching, unless as a teaching aid or in an emergency.

7.4. Mobile phones, or devices with imaging or sharing capabilities, must never be used in an area where pupils or staff might change or be in a state of undress, except in an emergency. In such an event, this must be reported to a DSL.

7.5. Pupils should use the school wifi at all times when accessing the internet at school, and so should not attempt to use 3, 4 or 5G, or a VPN to circumvent the schools filtering and monitoring system.

7.6. No one should bring any content into school on their device which is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).

7.7. In addition to the above, personal mobiles or personal devices with imaging or sharing capabilities, must not ever be used to record activities of pupils in EYFS. School devices are provided to record photographic evidence for pupil achievement or for marketing purposes.

7.8. All calls to staff regarding school business should where possible be directed through the main school telephone number or using School devices. Housemasters/mistresses and Heads of Section have school mobile phones or use the Google Voice app on their personal mobile phone when making or receiving phone calls for school business.

7.9. Whilst it is recognised that members of staff may need or choose to use their own telephone to contact each other, staff are advised that contact with parents should, wherever possible, be undertaken through the school telephone system.

7.10. Parents should be discouraged from contacting members of staff on their personal mobile phones.

7.11. 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.

7.12. 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.

7.13. 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.

7.14. 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.

7.15. Use of devices by parents is covered in taking, storing and using images of children policy.

8. MONITORING AND ACCESS

8.1. 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 Google 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.

8.2. Any personal devices used by pupils, whether or not such use is permitted, may be confiscated and examined under such circumstances. The school may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy.

8.3. Younger children in the prep school and, in particular EYFS, will be closely supervised when using devices within school to ensure they are accessing safe and appropriate sites only.

8.4. All pupils and staff are required to sign an annual declaration that they will abide by the rules and restrictions as laid out in the relevant documents. The pupil declaration included a simplified version of the information laid out in this policy, at an age appropriate level. Both the Prep and Senior School declarations can be found in appendix 1 (Prep) and appendix 2 (senior).

8.5. The recording, monitoring and filing of reports in the event of a potentially unsafe or inappropriate online incident are detailed under CPOMS where action will be taken by the DSL to address mitigations to avoid future repetitions of the same or similar incidents.

8.6. All necessary actions are taken to minimise the risk of any identified unsafe or inappropriate online incidents reoccurring.

8.7. Any current issues are discussed at relevant DSL, BMT, ELT and SLT meetings and any required changes to filtering controls actioned accordingly.

8.8. Effective training and online safety advice is available to all teachers and EYFS practitioners through Educare. This includes advisory support to children, young people, parents and carers as necessary.

8.9. In common with other media such as magazines, books and DVDs, some material available via the Internet is unsuitable for children and young people. We will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer.

8.10. Oswestry School cannot accept liability for the material accessed, or any consequences of internet access but will uphold high standards to try to prevent it.

8.11. If a child or young person accidentally accesses inappropriate material, it must be reported to an adult immediately. Appropriate action should be taken to hide or minimise the window. The computer should not be switched off, nor the page closed, in order to allow investigations to take place. All such incidents must be reported to the DSL; who must ensure a report of the incident is made and that any further actions deemed necessary are taken.

8.12. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

9. TRACKING DEVICES AND TECHNOLOGY

9.1. The school is not responsible for individual settings on personal devices, nor for the use of tracking apps/devices for purely personal and domestic purposes.

9.2. Use of this technology in the context of school activities is not specifically encouraged but if parents do plan to use it then they should be aware of potential third-party privacy considerations and only use it for domestic/personal purposes in respect of their own child and/or their or their child's belongings.

10. MANAGING EMAIL, WEBSITE AND SOCIAL MEDIA CONTENT

10.1. Written permission from parents or carers will be obtained before photographs of children and young people under the age of 16 are published on the school's website

10.2. Full names of children and young people should not be used anywhere on the website, first names will only be used in association with photographs

10.3. Where audio and video are included (e.g. Podcasts and Video Blogging) the nature of the items uploaded will not include content that allows the children and young people, under the age of 16 to be identified

10.4. The school will take overall editorial responsibility and ensure that content is accurate and appropriate

10.5. The school will promote safe use of e-communications to other practitioners, professionals, parents/carers, children and young people

10.6. Children and young people should immediately report to an adult if they receive offensive emails

10.7. Children and young people should not reveal any details of themselves to people they do not know, such as an address or telephone number, or arrange to meet anyone

10.8. Younger children in EYFS and KS1 will not be provided with individual accounts for email.

10.9. Young people should use email in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of appropriate conduct and may be classed as bullying

10.10. Emails sent to an external organisation should be written carefully and authorised by line managers before sending, in the same way as a letter written on headed paper.

10.11. The teaching of Online Safety will be part of the provision for all children and young people. It will include key messages that are age and maturity appropriate, such as keeping personal information safe, dealing with cyberbullying, knowing who to tell if there is inappropriate content/contact on-line

11. COMPLIANCE WITH RELATED SCHOOL POLICIES

11.1. You will ensure that you comply with the school's Online Safety Policy, BYOD policy, taking, storing and using images of children policy, Data Protection policy, Privacy notices, anti-bullying policy, Safeguarding and other associated policies, health and safety policy and the School Rules.

12. RETENTION OF DIGITAL DATA

12.1. Refer to the School's General Privacy Notice.

12.2. Staff and pupils must be aware that all emails sent or received on school systems will be routinely deleted after 1 year of staff leaving the School or 25 years from the pupil's date of birth.

12.3. Any information from email folders that is necessary for the school to keep for longer, including personal information (e.g. for a reason set out in the school privacy notice), should be held on the relevant personnel or pupil file. Important records should not be kept in personal email folders, archives or inboxes, nor in local files. Hence it is the responsibility of each account user to ensure that 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.

12.4. 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 Headmaster.

13. BREACH REPORTING

13.1. Refer to the School's Data Protection Policy

13.2. 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.

13.3. 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:

13.3.1. loss of an unencrypted laptop, USB stick or a physical file containing personal data;

13.3.2. any external hacking of the school's systems, eg through the use of malware;

13.3.3. application of the wrong privacy settings to online systems;

13.3.4. misdirected post, fax or email;

13.3.5. failing to bcc recipients of a mass email; and

13.3.6. unsecure disposal.

13.4. 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.

13.5. If either staff or pupils become aware of a suspected breach, complete the form on the Osnet homepage which automatically reports the Breach to the Privacy and Compliance Officer.

13.6. Data breaches will happen to all organisations, but the school must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The school's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will

not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

14. BREACHES OF THIS POLICY

14.1. A deliberate breach of this policy will be dealt with as a disciplinary matter using the school's usual procedures. In addition, a deliberate breach may result in the school restricting your access to school IT systems.

14.2. If you become aware of a breach of this policy or the Online Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to the Designated Safeguarding Lead. Reports will be treated in confidence.

ACCEPTANCE OF THIS POLICY

Please confirm that you understand and accept this policy by signing below and returning the signed copy to your form tutor/admissions (pupils) or HR (staff).

I understand and accept this acceptable use policy (staff / senior school pupils):

Name: ……

Signature: ……

Date: ……

For younger pupils (below secondary school age)

Name of parent/guardian: ……

Signature: ……

Date: ……

Appendix 1

These guidelines are in place to help you get the most from your devices and protect you from potential harm. In order to access the internet at Oswestry School Prep, you must agree to abide by them.

All Children

- All children at Oswestry School Prep access the internet as a normal part of their learning.
- If your child ever receives anything which upsets them through their school internet connection, they should report this to their teacher or another member of staff as soon as possible.

Children from Year 3-6

- Children from Years 3 - 6 are welcome to bring their own laptop or similar device into school with them.
- Children should take sensible steps to protect their device by using a password, PIN or pattern to enable/disable access to your device.
- Children are responsible for their devices at all times in school. They should be put in a protective case when they are not using it. If their device becomes damaged, lost or stolen, they should inform an adult immediately.
- Children must not use their device to record or take pictures of anyone on the school site or on school transport, especially without their permission. If they become aware of this happening, they must let an adult know immediately.
- Children are not permitted to carry mobile phones in school. Phones may only be used by Bellan pupils when travelling on school transport to and from school if the SIM card has been removed by parents to disable any connectivity to the internet. Any phones must be handed in to Form Teachers (or bus drivers) at the start of the day.
- Children must use the School's BYOD wifi to connect to the internet while at School or another of the schools wifi networks if a member of staff tells them to. Pupils must not use VPNs to circumnavigate the School's WIFI or filtering system.

Children should be logged onto their Oswestry School account whenever they are using the internet.

Appendix 2

Pupil Safe Use of Internet Agreement

These guidelines are in place to help you benefit from technology and adherence to them will also protect you from potential harms associated with the use of electronic devices while in school.

- All Senior school pupils are expected to have a suitable and working device with them at all times in school.
- You should take sensible steps to protect your mobile device by using a password, PIN or pattern to enable/disable access to your device.
- You are responsible for your devices at all times in school. Try not to leave them unattended or in insecure places. If your device becomes damaged, lost or stolen, inform reception or a member of staff immediately.
- You must not use your device to record or take images of anyone on the school site, especially without their permission. This is particularly forbidden in places that are used for getting changed. If you become aware of this happening, you must inform a member of staff immediately.
- Pupils must use the School's wireless network to connect to the internet while at School. You should also not bring into School any previously downloaded content that is inappropriate on your device.
- Pupils using VPNs or mobile data to circumnavigate the School's WIFI or filtering system, should expect to be sanctioned and could have their I.T privileges temporarily removed.
- Our filtering system is there to protect you from directly or indirectly accessing inappropriate or harmful content.
- If you ever receive inappropriate content through your school internet connection, you should report this to the School's Designated Safeguarding Lead or another member of staff as soon as possible.
- Please sign and complete the form to confirm that you understand and accept this policy.