Media Policy

Introduction

This policy outlines the standard Westfield School requires users of the school systems to observe, the circumstances in which the school will monitor use of these systems and the action the school will take in respect of breaches of these standards. The school's users are expected to have regard to this policy at all times to protect its electronic communication systems from unauthorised access and harm.

The objective of this policy is to define the standards of conduct when employing the use of school and non-school owned electronic devices such as laptops, tablets, smart phones and other devices used to access the internet and school learning resources. It is also to safeguard those who use these resources both internally and externally and to ensure our resources are protected from deliberate or unintentional misuse and damage. Some of the required protection is provided automatically by our systems, for example a filtering system to protect persons using the internet; other safeguards depend upon users following these guidelines. Therefore our equipment and materials, and the usage of personal media devices within school grounds and on associated school events, will only be available to those who agree to follow the rules set out in this policy. Breaches of this policy will be taken seriously and any users found guilty may be subject to disciplinary action.

1 Legislative Framework

The use by pupils of the School's network systems and personal devices within school time is likely to involve the processing of personal data and is, therefore, regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code, issued by the Information Commissioner. The school is also required to comply with the Regulation of the Investigatory Powers Act 2000, the Telecommunications Regulations 2000 and the principles of the European Convention on Human Rights incorporated into the United Kingdom law by the Human Rights Act 1998.

2 Personnel Responsible for Implementation of Policy

2.1 The School's Governing Body has overall responsibility for this policy but has delegated day-to-day responsibility for overseeing and implementing action to the Headmaster. Responsibility for monitoring and reviewing the operation of this policy lies with the ICT committee in conjunction with our service provider, Adept.

2.2 All users have a specific responsibility to operate within the boundaries of this policy, to facilitate its operation by ensuring that they understand the standards of behaviour expected of them and to identify and act upon behaviour falling below these standards.

2.3 All users are responsible for the success of this policy and should take the time to read and understand it and to disclose any misuse of the systems to a member of the Senior Leadership Team.

3 Who is covered by this policy

The policy covers all users of the school and also third parties who have access to the School's electronic communication and network systems.

4 User Owned devices and Bring your Own Device

4.1 If you wish to bring your own device and use it in school you must submit a completed BYOD contract to the Headmaster's PA. The school reserves the right to refuse to allow access to particular devices or uses where it considers there is a risk to the school network.

Last reviewed by Mr J Leese on 7 September 2021 and ratified by the Board of Governors on 21 October 2021

4.2 Users should not, under any circumstances, access our network resources on their own device without signing our BYOD Contract. The school reserves the right to remove your device at anytime if you are seen to be violating this policy or any other related school policy.

4.3 The BYOD policy and pupil contract covers access to the internet through our wireless network provision and the pupil's own internet provider. It gives permission for Sixth Formers to use their own device(s) under the provision of the policy at all times during school hours and other Senior House pupils with subject teacher permission during class time if they have successfully submitted a BYOD contract.

4.4 The school requires that users have installed anti-virus software available for that device. The school does not guarantee provision of anti-virus software for BYOD.

4.5 Where a user uses their own device to access and store data that relates to Westfield School then it is their responsibility to familiarise themselves with the device sufficiently in order to keep the data secure. In practice this means preventing theft and loss of data, where appropriate keeping information confidential and maintaining the integrity of data and information. Users should delete sensitive emails once they have finished with them and delete copies of attachments to emails on their own device as soon as they have finished with them.

4.6 In the event of loss or theft a user should change the passwords to all the school's services accessed from that device and report the loss or theft within 48 hours to the Bursar.

4.7 When a device has been registered and approved the device can be connected to the school network via access with the wireless password. Users are not permitted to share this access key or password with anybody else. If a user is found to have given this access key to anybody, their access to the system will be revoked and disciplinary action taken. The user's device will be issued with a monitored IP address. Users are not permitted to edit, adjust, mask or share the IP address they have been given.

4.8 Users are not permitted to use any device to create a wireless hotspot. Bluetooth should be disabled at all times while on school premises.

5 Monitoring of User Owned devices, internet and Systems

5.1 The school will not monitor the content of user owned devices but will monitor traffic over the school system to prevent threats to the school network systems. The school will also monitor the school's name across all social media and online channels to look for any possible misuse of the school's name or abuse of the school or any member of the school community.

5.2 The school does not collect or store any passwords or personal information (except the MAC address of the device when connected to the school's wi-fi) when a UOD (user owned device) is connected to the internet.

5.3 The school may require access to a user's personal device whilst investigating cases of policy breach including, but not limited to, cyber bullying, hacking of the system or virus attack. The Headmaster may require access to a user's personal device whilst investigating any behaviour or allegation relating to our School Anti-Bullying or Disciplinary Policy. In these circumstances every effort will be made to ensure that the school does not access private information of the user which does not relate to the investigatory matter.

5.4 Controlled assessment on User Owned Devices should only be carried out under direct instruction from a head of department. Controlled assessment procedures and policies apply to all work completed on a user device. You must seek specific permissions to complete any controlled assessment on your own user device. OFQUAL policies, contract and guidelines apply to all coursework completed on any device.

5.5 Use of personal devices during the school day is at the discretion of the staff. Pupils must use devices as directed by their teachers.

5.6 The primary purpose of personal devices at school is educational or related to educational experiences.

5.7 The school will monitor websites visited though our wireless network. Monitoring will only be carried out to the extent permitted or required by law and as necessary and justifiable for the school purposes.

5.8 The school systems provide the capability to monitor telephone, e-mail, voicemail, web and other communications traffic. In order to perform various legal obligations in connection with its role as a school, use of its systems including the computer systems and any personal use of them, is monitored by the service provider and appropriate staff.

5.9 The school reserves the right to retrieve the contents of messages or check searches which have been made on the internet for the following purposes: in order to safeguard pupils and staff, to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy, to find lost message or to retrieve message lost due to computer failure, to assist in the investigation of wrongful acts and to comply with any legal obligation.

5.10 The School's policy is that complaints, gossip or rumour about the school or a member of the school community will be investigated. Where they relate to the use of websites or social media the School reserves the right to use inspection software to view web pages. This right will only be exercised when considered by the Headmaster to be necessary and reasonable in the interests of welfare and, in each case, a decision to view web pages will be balanced against the user's right to respect for private and family life.

5.11 Users will be held personally responsible for all material they have placed on a website or social media and for all material that appears where they are the host or account holder. Material of a threatening, abusive, bullying, racist, harassing or defamatory nature, whether placed during or outside school time (including the holidays) will be treated as a serious breach of school discipline.

6 Acceptable Media Usage

Acceptable Media Use applies to all Westfield School employees, pupils and parents. It is not meant to be an exhaustive list of what pupils and staff can or cannot do, and, it is expected that over time it will change and we welcome suggestions for improvement from pupils, parents and staff. It is our guide for responsible media usage.

6.1 Pupil use of device camera or microphone functions on school premises, including school events, functions and visits, is prohibited unless approved by a staff member. Pictures, video or sound recordings taken in school may only be used in school related learning and must not be posted, uploaded or shared on any website or system (e.g. social media) other than one that belongs to or is approved of by school. We would highly recommend that any school related media is stored on the school system.

6.2 It is prohibited to use your device to take pictures, video, sound recordings of any pupil or staff member without their permission. Failure to comply will be considered a disciplinary matter.

6.3 It is a user's responsibility to keep their device safe while at school, on school related visits and school sponsored activities. The school, governing body and staff at Westfield School are not responsible for any damage, loss, malware or theft of a user device (including any such event which causes the device not to function). It is the user's responsibility to ensure that they have sufficient personal high value insurance to adequately cover the device for any such occurrence.

6.4 It is a user's responsibility to ensure their device is charged for the school day. The school does not provide electrical outlets that can be used by users for charging devices. If a user is found to be using an electrical outlet for charging their device then the charging device may be removed and can be collected at the end of the school day.

6.5 The school does not provide support for user owned devices. Users should be competent in the use of their own device. The school does not provide direct printing from users' own devices.

6.6 All school provided equipment and resources are provided for "acceptable" school use only and should not be used for personal tasks.

6.7 When using any equipment you must not behave in a way that could cause damage to the equipment or jeopardise our licensing agreements and/or conditions.

6.8 You are responsible for the safety of your account information; under no circumstances must you share your details with others, including family members, or let them use your account. You are also obliged to remember your user name and password and keep that information secure. You are required to change your password at least once a term.

6.9 You must not knowingly violate the privacy, or personal rights of other users. Examples of this type of behaviour would include (but not to be limited to) reading their mail, accessing their files or social networking sites, using their computer account or additional resources that they may have been allocated.

6.10 When accessing the internet through both hard and wireless networks on either a school or personal media device within school property, you may not deliberately access sites which may contain illegal materials, obscene or pornographic content, or which may be deemed offensive, threatening or abusive. The use of sites which contain games, chat rooms and cheats are expressly prohibited. You must immediately inform a member of the Senior Leadership Team if you accidentally access a site which contains any of the above information.

6.11 You accept that any work created using the school resources, including information sent or received by email, remains the property of Westfield School and may be accessed at any time for audit. You therefore agree not to use any form of private file encryption or make any effort to hide material.

6.12 You will not knowingly perform any act which may cause technical disturbance to the network, including the introduction of viruses, worms or any other destructive mechanism. You are expected to take any reasonable precautions such as not opening emails from an unknown source, using memory sticks or CD ROMs.

6.13 You may never copy, or allow to be copied, software, applications or data (including media images without permission) from school systems to another person or onto another system.

6.14 When using the resources available, including email, messaging systems and social network sites, you must not store or transmit any images of other pupils or staff, or use any statements that may be deemed offensive, threatening or abusive.

6.15 You may not perform, or take part in, any act which may create, transmit, distribute or store material that violates a trademark, copyright or any other intellectual property rights, this includes (but is not limited to) the use of pirated software or material downloaded from the internet. Also you may not encourage any conduct that would constitute a criminal offence or give rise to civil liability.

6.16 Any conduct which violates the Media Policy or any other conduct which is deemed inappropriate will be investigated. If a user is found to be at fault any or all of the following sanctions may be imposed: Restricted network access, disciplinary action, confiscation and retention of devices used (including mobile and all media devices), should there be reasonable suspicion of misuse. If a user is found to be responsible for the damage of equipment – a contribution up to the full cost of repair or replacement will be required. If it is suspected that a user has committed a criminal offence this will be reported to the relevant authorities for further investigation.

7 Incidents and response

Where a security incident involving users using their own devices arises at school this matter will be dealt with very seriously. The school will act immediately to prevent, as far as reasonably possible, any further harm occurring.

8 Data encryption Policy

The school issues all pupils with their own personal school email address. Access is via personal LOGIN, which is password protected. The school gives guidance on the reasons for always logging off and for keeping all passwords securely.

9 Promoting Safe Use of technology

9.1 The school adheres to best practice regarding e-teaching and the internet. Westfield recognises that internet safety is a child protection and general safeguarding issue.

9.2 The whole school supports the annual Safer Internet Day. Pupils of all ages are encouraged to make use of the excellent online resources that are available from sites such as:

- UK Council for Child Internet Safety (http://www.education.gov.uk/ukccis)
- Childnet International (www.childnet-int.org)
- Cyber Mentors (www.cybermentors.org.uk)
- Cyberbullying (www.cyberbullying.org)
- E-Victims (www.e-victims.org)
- Bullying UK (www.bullying.co.uk)

9.3 Users prepare their own models of good practice, within curricular lessons. They cover the different hazards on the internet, such as grooming, stalking, abuse, bullying, harassment and identity theft. Guidance covers topics such as saving oneself from future embarrassment explaining that any blog or photograph posted onto the internet is there permanently. Anything that has been deleted may be cached in a search engine, company server or internet archive and cause embarrassment years later.

9.4 Our designated safeguarding lead (DSL) has been trained in the safety issues involved with the misuse of the internet and other mobile electronic devices. The DSL receives regular monitoring reports of internet usage. They work closely with Newcastle Safeguarding Children Partnership (NSCP) and other agencies in promoting a culture of responsible use of technology that is consistent with the ethos of Westfield School. All of the staff have also received training in e-safety issues. The school's has a comprehensive PSHEE programme on e-safety. The PSHEE co-ordinators will ensure that all year groups in the school are educated in the risks and the reasons why they need to behave responsibly online.

9.5 With the explosion in technology, the school recognises that blocking and barring sites is no longer adequate. Westfield teaches all of its pupils to understand why they need to behave responsibly if they are to protect themselves. The school's technical staff have a key role in maintaining a safe infrastructure at the school and in keeping abreast of the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of ICT.

9.6 The school's guidance is that pupils and staff should always think carefully before they post any information online. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

9.7 The school offers guidance on the safe use of social networking sites and cyber bullying in PSHEE lessons which covers blocking and removing contacts from 'friend lists'. The school's PSHEE lessons include guidance on how pupils can identify the signs of a cyber-stalker and what they should do if they are worried about being harassed or stalked online. The school offers guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe.

9.8 Westfield School seeks to work closely with parents and guardians in promoting a culture of e-safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school. The school recognises that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home

10 Cyber Bullying

10.1 Westfield School will not tolerate any illegal material and will always report illegal activity to the police and/or NSCP. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our anti-bullying policy.

10.2 Cyberbullying is a particularly pernicious form of bullying because it can be so pervasive and anonymous. There can be no safe haven for the victim who can be targeted at any time or place. The school's anti-bullying policy describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying.

10.3 Westfield School values all of its pupils equally. It is part of our ethos to promote considerate behaviour and to value diversity. Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and he or she should not be afraid to come forward.

10.4 The school expects pupils to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face-to-face contact.

10.5 Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. The school's anti-bullying policy is set out in the Handbook. The school is strongly committed to promoting equal opportunities for all, regardless of race, gender, gender orientation or physical disability. All pupils are encouraged to look after each other and to report any concerns about the misuse of technology or worrying issue to a member of the pastoral staff

11 Related Policies and contract appendix

Related policies and documentation

1. Anti-Bullying Policy
2. Controlled assessment policy and guidelines
3. OFQUAL controlled assessment guidelines
4. BYOD Acceptable Use Agreement