OSSETT ACADEMY

CREATING OPPORTUNITIES. ACHIEVING EXCELLENCE.

ONLINE SAFETY AND ACCEPTABLE USE POLICY

Recommended by: **Date:**	Standards Committee November 2017
Approved by: **Date:**	Full Governors November 2017
Review Date:	November 2019

CONTEXT

Ossett Academy have an obligation to provide safe and secure access to internet services. This policy, in addition to the staff and students acceptable use statements, is designed to protect the interests and safety of the Ossett Academy community.

All staff, students and visitors need to read and understand this policy before using Ossett Academy's IT Facilities and associated systems.

Applicable Acts of Parliament

- The Regulation of Investigatory Powers Act 2000 (RIPA)
- The Prevent Duty 2015
- Data Protection Acts 1988 and 2003
- The Computer Misuse Act 1990
- Keeping Children Safe in Education (2016 Statutory Guidance)

Referenced Ossett Academy Material

- Behaviour Policy
- Data Protection Policy
- ICT Acceptable Use Statement – Student
- ICT Acceptable Use Statement – Staff
- ICT Bring Your Own Device Policy
- Social Networking Policy
- Disciplinary Policy

PARENTAL INVOLVEMENT

Parents/carers are asked to read through the Acceptable Use Policy and sign the acceptable use statement on behalf of their child on admission to the Academy. Failure to sign the acceptable use statement may lead to their child having no access to internet sites.

Ossett Academy promote online safety information to parents using the following methods:

- On student Admission to Ossett Academy
- Parents/Progress Meetings
- Ossett Academy Website and Android/iOS App
- Newsletters

Any complaints, concerns or queries regarding this policy or a child's online safety should be directed to the Ossett Academy safeguarding team.

USER AND ACTIVITY MONITORING

Internet Monitoring and Reporting

Ossett Academy constantly log access to websites and external systems via different levels of firewalls and networking devices hosted onsite. These logs are monitored and reported on both manually and proactively to detect issues relating to security/misuse, child protection and the Prevent Duty.

Ossett Academy decrypt and log access to secure sites (SSL encrypted). There is no intention to decrypt usage of the following categories of site, however monitoring of access does occur:

- Financial Services (Internet Banking)
- Government Websites
- Webmail

Internet Filtering

Ossett Academy block and monitor access to categories of website in line with goverment guidelines. Categories which are blocked are listed below:

- Adult Themes (adult humour, bad language etc)
- Adverts and Tracking Sites
- Child Abuse
- Criminal Activity
- Drugs and Alcohol
- Gambling
- Gore
- Intolerance
- Malware and Hacking
- Online Games
- Piracy and Copyright Infringement
- Plagiarism
- Pornography
- Social Media (apart from specific allowed pages)
- Social Networking
- Steaming Video – Pay to View (Netflix, Sky Go etc.)
- Terrorism
- Timewasting Sites
- Violence
- Weapons

Device Monitoring

Device Monitoring is performed differently on each category of device and can change without notice. Teachers may monitor devices in real time during lessons to give students one to one help, monitor usage and monitor behaviour in the classroom. IT Support use device monitoring to troubleshoot technical issues and to train staff/students on how to perform user based operations when required.

Due to the nature of device monitoring, there may be times when a screen is monitored in real time by a teacher or IT Support. In this case, the initiator of the monitoring cannot guarantee what information is already open on the device and for that reason privacy cannot be guaranteed.

Mobile phones and tablets enrolled under Ossett Academy's Bring Your Own Device service are subject to the **Bring Your Own Device Policy**. Specific, additional device monitoring is performed and discussed under that agreement.

Ossett Academy reserve the right to remotely wipe or disable an Ossett Academy owned device in the event of theft, loss or possible data security issues. This will only be done by the IT Support Manager with authorisation from a Senior Leader.

Sharing of Internet and Device Activity

Ossett Academy will comply with legitimate and lawful requests from Government agencies regarding specific user activity. Any request for information must be authorised by the Principal of Ossett Academy.

UNACCEPTABLE USE

Under no circumstance is a member of staff or student authorised to engage in any illegal activity using IT facilities or systems at Ossett Academy (applicable by UK or International law).

In Addition, the following activities are strictly prohibited.

- Creation or replicating malicious programs (virus, spyware, ransomware, adware)
- Sharing personal usernames/passwords with others
- Unauthorised copying or sharing of copyright materials (such as photos, music, documents, books etc.)
- Unauthorised installation of copyright material (games, applications etc.)
- Hacking, manipulating or unauthorised modifying of network security in order to access data or cause damage to software/hardware systems.
- Port scanning, network monitoring/interception and penetration testing is prohibited unless authorised by IT Support
- Sharing Ossett Academy software, data or sensitive information outside of the organisation without prior consent
- Sending unsolicited email messages (junk mail, phishing, spam etc.)
- Signing up to websites/services using Ossett Academy's name without prior consent from IT Support
- Providing sensitive unencrypted data to an external entity

The list above is not exhaustive and it's expected that staff and students at Ossett Academy use a good standard of morals and ethics to go about their daily activities.

Email

Ossett Academy provide all staff and students with an email account which they should use to represent their position at Ossett Academy. The use of this email account is subject to the following rules:

Users should only use their Ossett Academy email account for work purposes

Staff must never use their personal email address for communication of Ossett Academy information or correspondence.

The email system is monitored and should not be treated as private. Ossett Academy reserve the right to access mailboxes for IT maintenance and safeguarding purposes. Ossett Academy also reserve the right to access work email accounts as may be deemed necessary for essential Academy business during periods of staff absence e.g. through long term sickness absence or extended periods of leave of absence. In all cases where

this is deemed necessary prior approval and/or notification will be sought from the member of staff.

Ossett Academy reserve the right to close down email accounts or temporarily disable access in the event of a security issue (i.e. unauthorised access to email, password hacking etc.)

Social Networking

Ossett Academy has a **Social Networking Policy** which covers acceptable use.

Peripherals and Accessories

The facility to plug in peripherals and accessories to Ossett Academy devices is possible providing approved in this policy.

Webcams, photography and Imaging devices

On admission to Ossett Academy, every parent/carer has the option to prevent their child's image from appearing on websites, internal systems and promotional material. This information is available to staff from SIMS or via the Data Office. All staff should be aware of the student status before taking photos or videos.

Webcams should only be used for video conferencing/calling (i.e. Skype) under the supervision of a teacher. Using personal accounts for video conferencing/calling is prohibited using Ossett Academy's IT facilities.

The teacher initiating/approving the video conferencing/calling session is responsible for keeping a record of all parties contact details involved in the session.

Permission must be sought from parents/carers if their children are involved in a video conference/call.

USB and Storage Devices

It's recommended that all staff use encrypted usb storage devices if transport of data is required to a 3rd party. Unencrypted devices are not banned but should only be used for lesson material which does not include data that identifies a student, staff or entity of Ossett Academy.

All data on USB devices is subject to anti-virus scanning and file level blocking whilst connected to an Ossett Academy device.

Under no circumstances should a storage device be left unattended and unsecured at any time. This violates the **Data Protection Policy** and could lead to serious disciplinary action.

Ossett Academy takes no responsibility for any damages incurred when using USB storage devices nor does it take any responsibility for loss of data on a USB storage device.

Mobile Phones, Music Players

No device capable of becoming a mobile hotspot, modem or internet access device for an Ossett Academy device should be connected via cable or wirelessly to an Ossett Academy device.

Music Players (iPods etc) may be connected for charging purposes or to play music via computer speakers.

Under no circumstances should a mobile device be left unattended and unsecured at any time. This violates the **Data Protection Policy** and could lead to serious disciplinary action.

Other Devices

Under no circumstance should any other portable accessory or peripheral be connected to an Ossett Academy device without prior consent from IT Support. For all devices not listed, a security risk assessment should be carried out by IT Support before allowing/disallowing.

PASSWORD SECURITY

Password Strength

All usernames and passwords should be of complex structure and should:

- Have at least 8 characters
- Have uppercase and lowercase letters
- Contain at least 1 number
- Contain at least 1 symbol
- Not form part or whole of the user's name or username
- Not have consecutive numbers or characters i.e. 1234 or rstu etc.

Shared Accounts

From time to time there may be a working requirement that more than one person share a password or user account. This should be approved by IT Support and auditing of account login/logout times should be performed by the individuals sharing the account. A shared account should only be used for the purpose it's designed for and access to all other systems should be performed under the user's individual account.

Password Disclosure

Users must not disclose their passwords to anyone.
Passwords should never be written down.

REMOTE ACCESS

Users have access to resources from most devices in most internet enabled locations. Ossett Academy reserve the right to block external access from systems known to be advertising suspicious behaviour or if an IP address/domain is linked to a criminal organisation/activity.

Users should ensure that their own devices have adequate security updates and anti-malware software installed prior to connecting.

Remote Desktop

Taking control of a virtual remote desktop can be achieved. This is designed to give staff access to resources from home. It's essential that staff ensure that this connection is performed in privacy and where no other person can view the screen.

Remote Access to Email

The same rules apply outside of the Academy to inside. Staff and students have access to this system.

Intranet/VLE

Ossett Academy operate an Intranet/VLE where resources can be accessed by staff and students via a web browser.

SIMS Learning Gateway

Staff, students and parents can access real-time information from home. As this system gives access to student information, users should ensure their device is secure and not viewable by any other person.

Anti-Virus and Anti-Malware

All Ossett Academy's Microsoft Windows and Apple Mac devices have adequate anti-virus and anti-malware software installed to protect against threats. If a user of a device finds a suspicious file, it should be reported directly to IT Support with urgency.

All Ossett Academy issued roaming devices should be connected to Ossett Academy's internal networks at least once every seven days in order to perform compliance, security and anti-virus checks. Failure to do so may result in the device being revoked.

Websites and Services

Websites and services which require a user to sign up to must first seek approval from IT Support to ensure the website conforms to data protection guidelines. IT Support may seek further advice or approval from the designated data protection leader depending on the circumstances.

UK laws restrict children under a certain age from being able to sign up to services, it's essential that staff are aware of this when using online services for revision/coursework etc.

Parental consent may also be required in some circumstances.

Signature: **Principal**	
Signature: **Chair of Governors**	
Date:	November 2017