Education 1st

"enhancing lives through education"

Sports 1st

Device, Google Drive and BYOD Policy

Policy Review

The responsibility of reviewing and maintaining this policy is Craig Dembicki (Managing Director). This policy will be reviewed annually.

Start date of policy: **2nd September 2015**
Last review date: **22nd July 2018**
Date of next review: **22nd July 2019**

Signed Date: 22nd July 2018

Craig Dembicki
Managing Director
Education 1st

Device Policy

Introduction

Mobile devices, such as smartphones, tablet computers and laptops, are important tools for Education 1st and their use is supported to achieve the company's aims including monitoring attendance, student profiles, facilitating learning, referral details, tracking progress and behaviour monitoring.

However mobile devices also represent a significant risk to information security and data security because if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorised access to the organisation's data and IT infrastructure. This can subsequently lead to data leakage and system infection.

Education 1st has a requirement to protect its information assets in order to safeguard its students and customers, reputation and personal data.

This document outlines a set of practices and requirements for the safe use of mobile devices both company and personally issued.

Scope of this policy:

- All mobile devices, whether owned by Education 1st or owned by employees, that have access to corporate networks, data and systems, including corporate IT-managed laptops. This includes Mobile phones and tablets.
- Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk assessment must be conducted being authorised by the leader for IT

Technical Requirements:

- Devices must use the following Operating Systems: Android 2.2 or later, IOS 4.x or later.
- Devices must store all user-saved passwords in an encrypted password store.
- Devices must be configured with a secure password that complies with Education 1st's password policy. This password must not be the same as any other credentials used within the organisation.

User Requirements

- Users must only load data essential to their role onto their mobile device(s)
- Users must report all lost or stolen devices to **The IT Manager** immediately
- If a user suspects that unauthorised access to company data has taken place via a mobile device the user must report the incident to the IT Manager immediately
- Devices must not be "jailbroken"* or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user
- Users must not load pirated software or illegal content onto their devices
- Applications must only be installed from official platform-owner approved sources
- Under no circumstances must social media apps or websites be accessed on devices owned by Education 1st
- Installation of code from untrusted sources is forbidden. If you are unsure if an application is from an approved source contact Education 1st IT department

- Devices must be kept up to date with manufacturer or network provided patches. As a minimum patches should be checked for weekly and applied at least once a month
- Devices must not be connected to a PC which does not have up-to-date and enabled anti-malware protection and which does not comply with corporate policy
- Devices must be encrypted in line with Education 1st's compliance standards
- Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify **IT Manager** immediately, if they are unavailable revert to your **line manager**.
- In the event that staff want a student to complete work by using the device, staff must demonstrate best judgement i.e. taking account of the mindset of the student and the environmental circumstances. It is staff responsibility to supervise student access and use
- Users must comply at all times with related Education 1st policies (e.g. Data Protection, ICT Acceptable Use, e- safety)
- Users must only log into their own assigned account. An deviation from this could result in disciplinary action

**To jailbreak a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorised software.*

Devices owned by Education 1st

- Education 1st requests and requires that staff using devices owned by the company to be returned when leaving employment in the same condition as they were received. The employee will be liable for the full cost of any device which has not been returned at the end of employment.
- Any damage that occurs as a result of negligence by the employee or whilst the device is in the employee's care will result in the liability of the employee who is responsible for the device (Device will be signed out at beginning of employment). This may include the need to place the device in a protective casing to avoid dents and scratches.
- In the event of unforeseeable circumstances that result in damage to a device whilst in the care of the employee, the company may accept a percentage of the costs of repair if it is deemed that it is liable to do so. (To be decided by the management team)
- Education 1st uphold the right to block employee access to any system and device if felt necessary and appropriate.
- Photographic content taken of children for educational or marketing purposes on devices owned and regulated by Education 1st must stay on the device until being emailed to john.birkett@education-1st.org.uk. Upon emailing this must be then permanently deleted. Under no circumstance is this to be downloaded or uploaded to any device other than the secure device regulated by Education 1st.
- All employees must sign a liability waiver before any Education 1st owned device has been issued

Google Drive Policy

Purpose

This policy applies to all employees in all departments of Education 1st, no exceptions.
This policy pertains to all external cloud services, e.g. cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc. Personal accounts are excluded.
If you are not sure whether a service is cloud-based or not, please contact the IT Leader.

Policy

- Use of cloud computing services for work purposes must be formally authorized by the IT Manager. The IT Manager will certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud computing vendor.
- For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the IT Manager.
- The use of such services must comply with Education 1st's existing ICT Acceptable Use Policy and BYOD Policy.
- Employees must not share login credentials with co-workers. The IT department will keep a confidential document containing account information for business continuity purposes.
- The use of such services must comply with all laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by Education 1st.
- The IT Manager decides what data may or may not be stored in the Cloud.
- Personal cloud services accounts may not be used for the storage, manipulation or exchange of company-related communications or company-owned data.

BYOD Policy

Purpose

Education 1st grants its employees the privilege of using a mobile phone of their choosing at work for their convenience. Education 1st reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below. This policy is intended to protect the security and integrity of Education 1st's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms. Employees agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

Acceptable Use

- The company defines acceptable business use as activities that directly or indirectly support the business of Education 1st.
- The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.
- Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the company.
- Employees must not use their own phone or device for taking photos/videos involving students without prior agreement with the Director of Learning.
- Devices may not be used at any time to:
    - Store or transmit illicit materials
    - Store or transmit proprietary information belonging to another company
    - Harass others
    - Engage in outside business activities
- Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc.
- Education 1st has a zero-tolerance policy for using any device while driving
- Students must not be given access to employee’s phones or personal data

Devices and Support

- Smartphones including iPhone, Android, Blackberry and Windows phones are allowed
- Connectivity issues are supported by IT
- Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

Security

- In order to prevent unauthorised access, devices must be password protected using the features of the device and a strong password is required to access the company network.
- The company's strong password policy is: Passwords must be a combination of at least 6 numbers
- The device must lock itself with a password or PIN if it's idle for one minute.
- After five failed login attempts, the device will lock. Contact IT to regain access.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Smartphones and tablets that are not on the company's list of supported devices are/are not allowed to connect to the network
- Smartphones and tablets belonging to employees that are for personal use only are/are not allowed to connect to the network
- Employees' access to company data is limited based on user profiles defined by IT and automatically enforced
- The employee's device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

Risks/Liabilities/Disclaimers

- While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- The company reserves the right to disconnect devices or disable services without notification
- Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy
- The employee is personally liable for all costs associated with his or her device
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, and/or other software or hardware failures, or programming errors that render the device unusable

Education 1st reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

Related Policies:

Child Protection and Safeguarding Policy
Confidentiality Policy
e -safety Policy
Data Protection Policy
ICT Acceptable Use Policy