EDGE GROVE

ICT Usage Policy

Related Policies and Documents:

- Safeguarding / Child Protection Policy
- Data Protection Privacy Notice
- Policy on Taking Storing and Using Images of Children
- e-Safety Policy
- ICT Device Issue and Release Form

Definitions

- **Devices** – Any authorised electrical or electronic device – data-containing or otherwise - which may be used by, connected to, or make use of The School Network.
- **The School Network** - Any and all Devices, facilities to interconnect and manage them, and services provided by them or to them by authorised third-parties, whether internal or external to the school.
- **Credentials** - Any and all provided information, access details, usernames, passwords, or access-control devices (e.g. smartcards, RFID tags, etc.), which can be used to gain access to the School Network.
- **Users** - Any and all authorised users of the School Network who possess such Credentials or use the School Network (including administrative staff, teachers, pupils and visitors).

ICT Usage

The School provides the School Network to Users so that they are able to perform necessary school purposes. Use of the School Network, and provision of the School Network and Credentials to Users is at the sole discretion of the School.

The School, as a necessary part of Safeguarding / Child Protection and Data Protection obligations, as well as basic security of the School Network, may record, monitor and limit any usage of the School Network – whether from an authorised Device or not. This may include, but is not limited to:

- Monitoring, recording and storage of all usage of School Network services access, Internet and emails, stored files and emails, and associated metadata (e.g. usage patterns, statistics, etc.).
- Blocking, filtering or otherwise preventing access to websites, emails, documents or other services or data.
- Withholding of permission to access, disabling, blocking or limiting of services or data on the School Network from Users or Devices.

Any such records may be kept for a reasonable amount of time, even after deletion by Users. The School reserves the right, at its sole discretion, to share this information or make public a complete listing of a User's activity to any requesting party to the extent permitted by law.

At all times, Devices provided by the School are considered the property of the School, unless otherwise made explicit. Data stored or generated on the network belongs exclusively to the School, and may be subject to the provision of the Data Protection Privacy Notice and relevant legislation, and the safeguards required for such data always apply. In particular, data which may be considered "Personal Data" under the terms of the Data Protection Act should never be taken off-site without both permission and suitable safeguards (e.g. encryption).

Users of Devices issued to staff will be required to sign acceptance of that Device and to use it under the terms of that acceptance.

The School will take reasonable steps to ensure that Data stored on the School Network is adequately secured and appropriate levels of back-up provided.

All Credentials supplied by the School are for a User's personal usage, unless stated otherwise, and in the execution of School business only. A User must never disclose any Credentials to other Users or to anyone else, or permit other people to use them, unless specifically authorised by the School (IT Manager) to do so.

All services and Devices provided by the School Network should be used only for School business purposes, in a professional manner (for example, email and online communication), and never for illegal activity (for example, copyright infringement).

Any and all additional Devices or software which are required on the School Network should be authorised by the IT Manager beforehand. Data recorded, generated, produced or derived from using any School Network device is considered school property, including photographs, videos, statistics, Credentials and documents. Unauthorised devices or software may be blocked, de-installed, disabled or otherwise prevented from using the School Network, and users may still have their actions monitored and recorded.

All Devices on the School Network – whether supplied by the School or merely authorised to use the School Network – are subject to the control of the security systems within the School Network. Specifically, it may be deemed necessary to enforce installation or de-installation of security or other applications, or the enforcement of settings on the devices, in order to ensure the integrity and security of the School Network. This may include, but is not limited to, anti-virus software, network management software, "group policy" restrictions, password policy settings, disabling or removal of malicious or unwanted software, disabling or removal of insecure features and other measures.

At all times, Users are expected to use the provided facilities reasonably and with regard to other Users. For example, Users should not unduly burden the School Network by, for example, downloading lots of large video streams simultaneously, or by placing large and unnecessary files into their allotted storage areas. This is especially important on shared resources, e.g. the Internet connection, shared storage (for example staff-only shares, or in email storage). Shared resources should not be used as a way to artificially increase personal resources for a single User (e.g. storing personal files on the shared storage to overcome storage limits).

Any unauthorised use of the School Network, or usage contrary to this policy, could result in the School taking disciplinary action. Any such violation may be considered Gross Misconduct. Any attempt to circumvent security controls in place on the School Network, or to obtain or continue access to Credentials, Devices or Data in an unauthorised manner is explicitly forbidden.

Upon cessation of access privileges to the School Network, or termination of employment, Users are expected to return all school-provided Devices, data and Credentials to the School.

Specific violations which are not permitted under the terms of this Policy could include:

- Giving your password or access card to a pupil, parent or other person, even temporarily.
- Allowing a pupil access to the School Network using a staff login – it is staff responsibility to ensure that they do not leave a PC or similar with an open connection to the Network.
- Otherwise providing data to pupils or parents without permission.
- Although "reasonable" personal use is permitted, "unreasonable" personal use of the Internet connection to browse websites is prohibited; if in doubt staff should check prior to use.
- Using the Internet connection for illegal purposes, such as downloading movies, software or other content not licensed to the school, or attempting to gain access to other computer systems without permission ("hacking").

- Circumventing school security measures, such as User permissions, security software, “Group Policy” or enforced device settings. This includes using another User’s Credentials to do so, uninstalling, disabling or interfering with the operation of security software, or otherwise obtaining access to School Network facilities that the User has not been authorised to use.
- Installing or attempting to install any unauthorised software (e.g. downloads from the Internet, CD-ROM’s, etc.) or Devices (e.g. USB “sticks” or other data drives, smartphones, scanners, printers, cameras, wireless network devices, etc.) without proper permission of the IT Manager.
- Using unlicensed, or improperly licensed, software on the School Network, even temporarily.

Working At Home

It is accepted that staff will access school personal data via their own home devices. Generally this involves access to emails, the MIS system and working on school documents. Staff must ensure that any personal data is treated with the same data confidentiality as if it were on the school site.

- Staff must never download and save documents to a private device that is not owned by them.
- Staff must ensure that personal data saved on their home device is secured by a password, fingerprint, pass code.
- Staff must ensure that school personal data is protected whilst in their own home and to/from the school and home. Papers must not:
    - be left in an unattended car,
    - be visible/accessible to non-Edge Grove staff – family, friends, visitors,
    - be disposed of in a home waste bin or recycling bin. Papers can be shredded at home or brought back to school for disposal.
- School personal data must never be sent to a non-Edge Grove email address including a staff’s personal email account, unless that email address has been approved by the Bursar, ie Governors, peri music teachers, activities staff.
- Staff should, wherever possible, access data via the following systems rather than emailing and downloading documents to their home device:
    - School Outlook/Emails http://mail.edgegrove.com
    - Firefly https://firefly.edgegrove.com
    - SchoolBase Online https://schoolbase.edgegrove.com
    - Google Drive https://drive.edgegrove.com
- If a document is saved to their home device, staff must ensure that it is deleted from the hard drive as soon as it is no longer required and deleted from their Recycle Bin.

Martin Sims
Bursar
April 2018

Appendix 1: Acceptable Use Agreement

Appendix 1

Staff, Governor and Visitor

Acceptable Use Agreement / Code of Conduct

IT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in School. This document is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. All staff are expected to sign the code and adhere to its contents at all times. Any concerns or clarification should be discussed with the School e-Safety coordinator (who will be the Head of IT) or IT Manager.

- I will only use the School's email / Internet / Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headmaster, Bursar or Governing Body.
- I will not browse, download, upload or distribute any material that could be considered by the School to be offensive, illegal or discriminatory.
- I will comply with the IT system security and not disclose any passwords provided to me by the School or other related authorities.
- I will ensure that all electronic communications with staff including those on social networking sites are compatible with my professional role.
- I recognise the potential implications of entering into any communication with pupils on social networking sites and that School policy strictly prohibits this. I agree to reject any "friend requests" that I might receive from pupils.
- I will only use the approved, secure email system(s) for any School business.
- I recognise the potential implications of data loss or mishandling and I will ensure that any personal data (such as data held on SchoolBase) is kept secure and is used appropriately, whether in School, taken off the School premises or accessed remotely.
- I will ensure that the Working At Home guidance is followed at all times so that any personal data is kept secure and disposed of appropriately.
- I will ensure that any device, including smartphones, tablets and laptops, regardless of ownership, which I use to connect to the School's email or internet or intranet systems will be protected by a pin code or password. Any laptop issued to staff by the School must be fully encrypted before leaving the School premises.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with published School policies (Policy on Taking, Storing and Using Images of Children and Appendix 3 of the Safeguarding / Child Protection Policy). The School holds a list of pupils whose photographs should not be used in Newspaper articles, the School website or in any marketing material.
- I will not attempt to install on or connect to the School network any hardware (including unencrypted USB sticks or Hard Drives), personal mobile phones, laptops, tablets or software without obtaining permission from the IT Manager.
- I understand that all my use of the Internet and other related technologies is liable to be monitored and logged and be made available, on request, to the Bursar or Headmaster.
- I will respect copyright and intellectual property rights.

I will support and promote the School's e-Safety and IT Usage policies and help pupils to be safe and responsible in their use of IT and related technologies.

User Signature: I agree to follow this code of conduct and to support the safe use of ICT throughout the School.

Signature …….……. Date ……..……

Full Name ……(printed) Job title ……..