Europe

Regional IT Policy

Version for Spain

September 2024

Contents

1 Introduction

The use of technology as a tool and enabler has become an integral part of school and home life. Cognita is committed to the effective and purposeful use of technology for teaching, learning and administration and is fully committed to protecting its staff (including contractors and peripatetic teachers), students, parents and visitors, collectiv from illegal or harmful use of technology by individuals or groups, either knowingly or unknowingly.

Cognita actively promotes the participation of parents to help the school safeguard the welfare of students and promote the safe use of technology.

This policy applies to the use of IT equipment, applications and services collectively nology (both on and off-site) that is supplied and/or made available to stakeholders via the school and/or regional office networks.

A copy of this policy is available on request and posted on the school website.

In the event of a breach of this policy, failure to have read this policy will not be accepted as a defence by any stakeholder. In such cases, Cognita reserves the right to investigate and take necessary action.

2 Policy Purpose

5 Safe Use of Technology

6 The Right to Use School and Office Network and Equipment

6.1. School employees and students will be allocated a username and password for accessing technology devices and services. They must **not** allow other individuals to use their account and shall not share any passwords with anyone.

6.2. School email accounts should only be accessed through Microsoft Office 365 or Google and all other third-party email services are **not** allowed.

7 Appropriate Use of Technology for Digital Safety

7.1. The school provides **System and Application Accounts** for stakeholders for educational and administrational purposes.

7.2. Stakeholders must **not**:

Allow

accompanying software unless under the written instruction of the SLT and/or Regional IT.

7.4. The school provides technology resources for accessing and storing data and has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare of stakeholders (further details in Appendix A-Web Filtering Statement).

Stakeholders must **not**:

Bypass website filtering
browser extensions and/or VPNs or similar systems) whilst using school devices whilst on and/or off-site
Access or attempt to access data for which they are not authorised
Interfere with digital work belonging to other users
Share private, sensitive and/or confidential information unless:

- they have authority to share
- the method of sharing is secure and does not use identifiers
- the recipient is authorised to receive that information
- there are safeguarding reasons (in which case only the Safeguarding team can share)

It is the responsibility of technology users when accessing data to be aware of Intellectual Property rights infringement including copyright, trademark, patent, design and moral rights.

7.5. The school endeavours to safeguard and where possible mitigate all **Security** risks associated with technology and will engage and collaborate with Regional IT, if required.

7.6. Concerns regarding any of the following must be reported to the Head or member of SLT who will, as required contact the Regional Safeguarding Lead and/or the Regional IT Team as soon as possible on the same day:

Access to unsuitable material/content on a school device or on the school network
Misuse of technology which has caused harm or abuse to another (or likely/potential to)-proportionately on a case-by-case basis
Concerns regarding viruses and other malicious software
Suspicious emails, links, and/or websites or any other communication

7.7. It is the responsibility of all technology users to ensure the **Welfare** of themselves and others both on personal and school devices. Stakeholders must **not**:

Use their own or the school's technology to bully

theoanv44 use w00.000008875 0 595.56 842.04 reW* nBT/F3 11.04 Tf1 0 0 1 179.33 206.66 Tm1643 Tm0 G[t)-4(he)3T0

Staff

performances/events organised by the school (and clear boundaries will be described).

9.6. Parents are asked to be considerate when taking videos or photographs at school events (with permission see above 9.5) and are requested not to publish material of other students in any public forum without the permission of the relevant family.

9.7. It is illegal to sell or distribute recordings from events without permission. Any parent who does not wish for their child to be videoed or photographed at school events by other attendees must notify the school in advance and in writing.

10 Use of School Equipment for Personal Use

10.1. School devices and IT systems are provided for school work and business purposes only; should a member of staff decide to use the equipment and/or IT systems for personal use, All concerns and incidents shall be reported to the Cognita Service Desk: servicedesk@cognita.com or via encourage prompt communication with the school so we can offer advice and support.

12.9. The school has a duty to report serious safeguarding concerns related to stakeholders to the authorities (Social Care/Services) or to the Police, in line with statutory requirements (see the Safeguarding Policy).

13 Removal of Network Access, Accounts and Devices

13.1. Anyone found breaching the IT Policy may have their network access, account(s) or device removed and may be subject to further disciplinary action.

13.2. The school and Regional IT

licence/authorisation from the to do so from the owner of the rights

15 Artificial Intelligence (AI)

15.1. Please refer to the **Cognita Statement on Artificial Intelligence in Education****

****As of June 2024, this statement is being re-drafted. The Regional IT policy will be updated following the re-draft and readers will be directed to the statement via a link.

16

ir outgoing email.

**To clarify, students can, and must

19 Appendix C - Related Policies

Europe & United States

- Safeguarding and Child Protection Policy
- Preventing Radicalisation Policy
- Behaviour Policy
- Code of Conduct Policy
- Personal and Professional Boundaries Policy
- Student Charter
- Data Protection Policy

Group IT

- Group Policy - Software (Applications)
- Cognita_Password_Policy.pdf
- Personal and Professional Boundaries Policy
- Cognita_Cyber_Security_Policy.pdf
- Cognita Safeguarding Systems_Cyber Security Policy

20 Appendix D - Related Online Resources

Department for Education (DfE)

- Keeping Children Safe in Education (KCSIE)
- Meeting digital and technology standards in schools and colleges
- Data Protection in Schools
- The Prevent Duty

Ownership and Consultation	
Document sponsor/approver	Head of IT Europe & United States
Document author	Head of IT Europe & United States
Consultation with	Europe Digital Learning Advisors
	Group Cyber Security
	Europe IT POD Leads
	Regional Safeguarding Lead (Europe and United States)
Audience	
Audience	Regional Employees
	Regional Students and Parents
	Suppliers
	Visitors
	Contractors
Document Application	
The policy is related to this jurisdiction	All Cognita Europe & United States Schools and Offices
Version Control	
Review cycle	Annual
Effective from	September 2024
Next review date	September 2025
Version	1.0 ISSUED