Cognita Europe IT Policy
Summary

Important notice

This document highlights the key messages from the Cognita Europe IT Policy. It is merely a quick reference sheet and does **not** negate a need to read the policy **in full**. Should an employee breach the policy (whether intentionally or otherwise), failure to have read the policy will not be accepted as a defence. In such cases, Cognita reserves the right to investigate and take necessary action.

1. Roles and Responsibilities

a. The POD General Managers (UK), Managing Director (Spain) and School Heads are responsible for sharing this policy and its ongoing implementation and monitoring at a school level.

b. All Cognita employees are responsible for adhering to the policy.

2. Safe Use of Technology

a. Use of technology must be legal, safe, responsible and respectful to others. Stakeholders are responsible for their actions, conduct and behaviour when using technology at all times.

b. It is each school's responsibility to educate students about the importance of safe and responsible use of technology to help protect themselves and others online. Regional IT support this via various resources, presentations and policies (including this one).

c. School teams should monitor students' use of school devices, whilst also undertaking random checks. Training is available to support staff to understand how to analyse the filtering data within Lightspeed.

d. Any concern regarding unsafe or inappropriate use of technology must be reported to a member of the SLT, Head of School or DSL/CPC or Cognita's Service Desk: servicedesk@cognita.com / +34936296806 on the same day of the identification of the concern.

3. The Right to Use School and Office Network and Equipment

a. Only school devices must be connected to the school network and personal devices should only connect to the guest network; if allowed by a member of the school SLT.

b. Students assigned a 1-to-1 device are required to sign the iPad/Laptop Usage Agreement (the link is in the Appendix of the Cognita EU IT Policy) and this shall be kept with the school.

4. Appropriate Use of Technology for Digital Safety

Stakeholders must **not**:

Hardware and software

1. Attempt to install unapproved software and/or applications onto school devices.

2. Remove, copy and/or attempt to alter the configuration of the hardware equipment or any accompanying software unless under the written instruction of the SLT and/or Regional IT.

3. Leave their device unlocked and/or logged into their account when not in use.

4. Bypass website filtering systems and/or technology security systems (via 'Tor' browsing, browser extensions and/or VPNs) whilst using school devices whilst on and/or off-site.

5. Access, create, store, share, download and/or upload illegal and/or inappropriate content as well as unapproved software.

Accounts

6. Use someone else's account and/or allow anyone to use *their* account unless authorised (in writing) by SLT and/or Regional IT.

Communication

7. Use mobile messaging apps to communicate with parents and/or students.

8. Send messages and/or emails from school accounts that purport to come from an individual other than the person actually sending the message.

9. Send work related messages and/or emails to/from a personal account.

10. Forward inappropriate content that they have received from a child, parent or staff member to any other child, parent, or staff member. Should they receive something of this nature, they must notify the DSL/CPC and Head immediately, who will seek advice from the Regional Safeguarding Lead. Staff must not delete the content until advised to do so.

11. Connect with students under the age of 19 on any social networking site or via personal mobile phones, or professional platforms. Should they receive a connection request they must not reply (please refer to the Code of Conduct).

Online etiquette

12. Use their own or the school's technology to bully others online, disrupt the learning of others and/or engage with people who they do not know.

13. Make offensive and/or inappropriate comments about the school and/or any parent or child associated with the school, on any forum/platform.

Information and data sharing

14. Access or attempt to access personal and/or commercially sensitive data for which they are not authorised.

15. 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).

5. Access and Privacy

a. School technology devices assigned to staff and students are for the sole use of the assignee.

b. To access another individual's assigned device, written permission must be given as follows (unless the access is required immediately for safeguarding reasons):

- Cognita HR Director or Partner for a device assigned to a member of staff
- The School Head for a device assigned to a student.

6. Photographs and Images

a. Schools must adhere to photo consent via the 'Use of Images' form.

b. Personal devices must **never** be used to take, store or share images of students.

7. Use of School Equipment for Personal Use

- Using work equipment and/or IT systems for personal use, is at your sole risk and could be considered as a breach of the Cognita Europe IT Policy.

8. Use of Personal Equipment in School

- Staff are permitted to bring a personal device on-site but must **not**:
    - use that device in the presence of students (please see Cognita Code of Conduct for Staff)
    - connect that device to a school network, only to the guest WIFI network
    - undertake work-related tasks on their personal device
- Students must **not** use a personal device on site unless they have *written* authorisation by a member of the SLT and/or Regional IT. Students must have an exceptional reason not to use their school supplied device.

9. Data Privacy Impact Assessment (DPIA)

a. Cognita performs a DPIA on applications, websites, software and services, collectively "third parties" where personal data is collected to ensure that the third party can be trusted with our data, and that we understand the risks of using the services. To find out more, please click here.

b. Only approved software and applications may be installed on a Cognita device or used via a browser as per this process. A list of approved third-parties can be found here.

10. Artificial Intelligence

- Please refer to the **Cognita Group AI Policy.**

11. Procedure for Reporting Concerns and Incidents

All concerns and incidents shall be reported to the Cognita Service Desk: servicedesk@cognita.com / 34936296806and appropriate members of staff depending on the concern/incident.

12. Resources

All users of technology may find the following helpful, in keeping themselves and others safe online: UK Safer Internet Centre / Internet Matters - resources / Google Family Safety / Common Sense Media