E-SAFETY GUIDANCE FOR STAFF

Date of Policy	August 2025
Next Review Date	August 2026
Key Staff	Senior Deputy Head, Deputy Head – Wellbeing, Designated Safeguarding Lead, Business Manager, School Systems Administrator, Dean of Student Experience
Lead for Review	Senior Deputy Head

Rationale

This policy outlines the expectations for staff at CATS Cambridge and CSVPA regarding the use of electronic communication and social media. It aims to minimise risks for both staff and students while ensuring a safe and professional online environment.

The 2024 KCSIE statutory guidance states that “all staff should receive appropriate safeguarding and child protection training (including online safety) at induction” and that the training should be regularly updated with staff receiving updates “at least annually”. It also states that “Online safety and the School's approach to it should be reflected in the child protection policy. Considering the 4Cs (Content, Contact, Conduct and Commerce) will provide the basis of an effective online policy”.

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation, radicalisation, sexual predation. Technology often provides the platform to facilitate harm. As educators, it is essential that we mitigate these risks towards staff by practicing safe working practices and protect and support both staff and students in our school.

An effective approach to online safety empowers a school to protect and educate the whole school community and their use of the technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

Security, Data and Confidentiality

- All users complete the necessary iHASCO training, read and agree to the Acceptable Use Policy to demonstrate that they have understood the school’s e-safety Policy during their induction process.
- When accessing, amending and saving any data or information, relating to the school or pupils, school staff follow the guidelines set out in the General Data Protection Regulations 2018.
- Use strong passwords and change them regularly. Protect your mobile device or computer with a PIN, especially when in school to prevent access to its content and potential misuse.

Managing the Internet

- Staff are responsible for all internet usage on their school laptop and mobile devices whilst on school premises.
- All internet activity within school is monitored and filtered.
- Whenever any inappropriate use is detected, the IT Manager and Vice Principal are notified, and the incident will be followed up in line with school policies.

Infrastructure

- Our internet access is monitored by our IT Manager and our ISP.
- All domain joined devices connected to the IT infrastructure at CATS Cambridge and CSVPA are administrated by the IT system administrators.
- Staff are aware that should they encounter or access anything unsuitable or damaging they must report it immediately to a member of SLT and the IT Manager.

Maintaining Professional Boundaries

- All communication with students must be professional, courteous, and formal.
- Only use official channels of communication e.g. school e-mail accounts or mobile phones and comply with CATS Cambridge/CSVPA Safeguarding and ICT policies.
- Staff must adhere to the School's Safeguarding and ICT policies:
    - Managing email: The use of email within school is an essential means of communication for staff. Staff must use the school's approved email system for any school business. Staff must inform (IT and their line manager) if they receive an offensive or inappropriate e-mail.
      Personal Mobile devices (including phones): The school allows staff to bring in personal mobile phones and devices for their own use. Staff must not use these to communicate with students/children.
    - All communication with stakeholders (staff, MDMs, agents, students and their families) must be done via either Outlook or MS Teams.
    - No sensitive information or images of students may be stored on personal devices.

The school is not responsible for the loss, damage or theft of any personal mobile device

Social Media and Personal Information

- Sharing personal information, including phone numbers, private email addresses, social media accounts, or personal photos, with students is strictly prohibited.
- Staff should politely decline friend requests or "follows" initiated by students on social media. Staff should not initiate such requests themselves.
- Friend requests from parents should be handled with discretion. It's acceptable to decline while reminding them of formal channels for discussing their child's education.
- Operate online in a way in which would not call into question your position as a professional.
- Realise that students will be naturally curious about your personal life outside school and may try to find out more about you

- Manage your privacy settings on all online accounts and keep them under review. These are particularly important in regard to photos, and remember that no privacy mechanism is 100% guaranteed
- Ensure your settings prohibit others from tagging you in any photos or updates without your permission and that you can ask others to remove any undesirable content related to you
- Consider that conversations held online may not be private. Be aware of who may have access to what you post
- Assume that information you post can be accessed and altered
- Do not discuss students, colleagues, parents or carers online
- Respect student privacy and confidentiality at all times but remain vigilant to indicators of safeguarding risks and report them appropriately

Safe Use of Images

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- All staff are aware of specific children in school who do or do not have photograph permissions. If they do have permission, staff are aware of the platforms they can be used on.
- All this information can be found on iSAMS or Shackleton. If in doubt, ask the DSL.
- Staff are encouraged to use the School's own mobile devices and cameras, to record images of pupils, this includes field trips. If personal digital equipment, such as mobile phones are used, the images should be appropriate, uploaded to the school network and then deleted immediately.

Publishing and storage of students' images and work

- All parents/guardians will be asked upon entry to the school to give permission to use their child's work/photos in publicity materials or on the school website, twitter account or mobile app.
- This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw or amend permission, in writing, at any time.
- Students' full names will not be published in association with their image and vice versa on Global Bridge, school media or any other school based publicity materials.
- Images/ films of children are stored securely on Global Bridge, the school server and / or teacher's individual school laptops.

Online Conduct

- Staff should always conduct themselves online in a manner that upholds their professional standing.
- Be aware that students may be curious about your personal life online.
- Privacy Settings and Online Security
- Manage and regularly review privacy settings on all online accounts, particularly regarding photos. Remember, no privacy setting is foolproof.
- Ensure settings prevent others from tagging you without permission and allow you to request removal of undesirable content.
- Remember that online conversations may not be private. Be mindful of who may have access to what you post.
- Assume all information posted online can be accessed and potentially altered.

Confidentiality and Reporting

- Never discuss students, colleagues, parents, or carers online. Respect student privacy and confidentiality at all times.
- Remain vigilant for potential safeguarding risks and report them appropriately to the DSL.

Cyberbullying

- Report any incidents of cyberbullying, or concerns about online comments, photos, or posts related to you or a student, to the DSL.

Minimising Student Risk

- Report any instances of risky or inappropriate online behaviour, social media use, or cyberbullying by a student (or concerning a student) to the DSL using the appropriate procedures.
- Educate students about safe and appropriate online behaviour.

Additional Measures

- Use strong passwords and change them regularly.
- Protect mobile phones, tablets, and computers with a PIN, especially on school grounds, to prevent unauthorized access and potential misuse.
- If staff have any additional questions or concerns regarding the use of external platforms such as Global Bridge or UpLearn, they can contact the DPO or ask the Senior Deputy Head to view the relevant DPIA.

Support

If you have any questions or concerns regarding this policy, please contact the Senior Deputy Head or DSL.

As a professional working in education, if you come across or are made aware of risky or inappropriate use of electronic communication, social networking or cyber bullying by a student or concerning a student report the matter to the DSL using the appropriate procedures. Alert your students to, and encourage them to, use appropriate and safe online behaviour