North Bridge House

Senior School

Cognita encourages open communication. It is imperative that you report any conduct that you believe to be inconsistent with our Policies as well as any unethical, unlawful or unsafe situations.

CONTENTS

1.0   INTRODUCTION

1.1 We define e-safety as:-

- ensuring student Internet use and access is appropriate and controlled.
- preventing misuse of Internet connected devices.
- ensuring students are educated on the risks carried with Internet use and how to minimise and deal with those risks.
- providing students with knowledge and resources to make decisions to ensure their safety online

1.2 Our core principles for e-safety are:-

- The Internet and Internet connected devices provide a rich resource for supporting teaching and learning.
- Our policies seek to educate and inform students and the school community on the safe and prudent use of Internet resources
- We take a whole school, consistent approach to E-safety, recognising that all staff should be involved and clear on their role in ensuring E-safety education.
- E-safety is subject to clear reporting routines and students are aware of how to report concerns.
- We recognise the need for regular training and ensure at least one member of staff takes accredited training and has a higher level of expertise.
- Our policy reflects current practice and is regularly reviewed and updated by the Lead Team and communicated to all staff.
- E-safety is addressed within the curriculum at all ages, including internet safety, cyber bullying, legal issues relating to copyright and the Misuse of Computer Act
- Technology in school is monitored to ensure it offers a safe access point to the Internet
- This policy should complement other school policies, in particular safeguarding policy; staff acceptable Internet and device use; data protection, anti-bullying or similar policies and student / pupil Acceptable Use of Technology Agreement.
- The e-safety policy and the information and guidance in the Pupil Planner is dated with a review date and it is reviewed and updated on an annual basis

2.0 WHOLE SCHOOL APPROACH

2.1 We take a consistent approach to E-safety and ensure that:

- All staff are aware of their responsibilities. E-safety procedures are discussed in induction for new staff. The policy and procedures are discussed in staff briefings and CPD sessions and training is provided at regular intervals.
- E-safety is mentioned on the SDP noting current state of practice and any areas for development.
- We ensure all students understand what is meant by E-safety through age appropriate delivery in the curriculum at all ages.
- All pupils are subject to a Commitment to Achieve: e-safety, which is signed by the students and discussed at the start of each new academic year.
- Parents are aware of their children's responsibilities and key information is shared with them
- Awareness raising events are held, such as assemblies, parent forums, PSHEE and Year Group assemblies
- The ICT Suite is protected by Web Sense and by Impero software. Impero allows for immediate blocks to be put in place if a gap is identified and logs all internet browsing history by username. In addition it flags potential violations live with alerts posted on the teacher's screen
- E-safety is raised as part of school council discussions
- There are notices and posters giving guidance on display in key areas of the school.

3.0 ACCEPTABLE USE OF TECHNOLOGY AGREEMENT AND REPORTING

3.1 We set out positive guidelines for how students should use and treat technology both during the school day and outside school as school representatives.

3.2 The acceptable use guidance is delivered to all students as part of the ICT Curriculum.

3.3 All pupils are asked to read and sign a Commitment to Achieve with regard to E-safety. This is presented to students in the Pupil Planner and therefore is available to

students joining the school later than the start of the academic year.

3.3.The Commitment to Achieve sets out the guidelines below:

COMMITMENT TO ACHIEVE – E SAFETY

I will follow the school contract for acceptable use of ICT and know that:

- the messages I send, or information I upload, will always be appropriate, polite and sensible
- sending malicious messages outside of school can become a matter whereby the school will set sanctions or involve outside agencies such as the Police
- if I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but will talk to a teacher or trusted adult
- I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk

We actively encourage in the classroom and around the school:

- appropriate and respectful use of school technology equipment and devices
- expectations and regulations for the use of students own devices in school
- expectations of behaviour if equipment is found broken or non-functional
- appropriate communications using devices in and out of school
- a clear code of practice if students discover inappropriate or upsetting material on any device so that they are aware that this can be reported online or by enlisting the help of a trusted adult
- clear guidance on how to report any concerns

3.4 We positively encourage appropriate and E-Safe behaviour and can be used alongside rewards for positive use of technology

3.5. These are a clear set of sanctions for when there are concerns about the use of technology. Sanctions are recorded in the Form Book and information is communicated to Pastoral and Academic staff and parents as appropriate. Records of any behaviour outside the agreement should be held, with clear description of the incident and sanctions applied

3.6 The E-safety policy is shared with parents and their views are welcomed and

considered.

3.7 The Commitment to Achieve – E Safety is not intended to form the whole basis of e-safety education, but to complement discussions and lessons on E-safety during curriculum time and to provide a robust agreement setting out clear expectations for behaviour along with the Acceptable Use Policy

3.8 The Commitment to Achieve – E-safety is designed to be binding for students while *enrolled* in the school and the school reserves the right to take action on behaviour that contradicts the Agreement outside of school time. In these cases the school will proceed with discretion and in partnership with parents.

3.9 Students, parents and all staff are able to report concerns.

4.0 STAFF AWARENESS AND TRAINING

4.1 All staff are bound by the code of practice set out in the Cognita Schools Policy for use of Internet and mobile devices. This is available for all staff and ensures that staff use technology safely and with adherence to safeguarding principles.

4.2 At least one member of staff should undertake accredited training. We recommend the Keeping Children Safe Online (KCSO) course provided by the CEOP. *This training is delivered online and is suggested to take 3 hours in total although it is not necessary for the course to be taken in one 'sitting'.*

4.3 The accredited member of staff should provide a higher level of expertise within the school and can guide staff in E-safety practice and review of E-safety policy and procedure and provide INSET guidance

4.4 E-safety is be built into the programme of meetings to ensure all staff are aware of their responsibilities and for the discussion of any issues, concerns or opportunities for events or cross curricular E-safety lessons.

4.5. There is a clear procedure for staff wishing to report or discuss concerns relating to E-safety or Internet access in the school. This procedure includes reporting to a member of the Senior Leadership Team and concerns should be documented as necessary.

4.6 Staff responsibilities for E-safety are: (for all staff)

- To ensure they are familiar with and fully support the student Acceptable Use of Technology Agreement
- To be vigilant when using technology as part of lessons
- To model safe and responsible use of school technology
- To provide reminders and guidance to students on acceptable use
- To report and act appropriately if they become aware of, or after any student reports, a concern or an incident involving technology use
- To ensure e-safety is delivered within the curriculum as appropriate to their student age range and subject area
- To contribute to and discuss e-safety policy and to have their views heard
- To be aware of the school policy for tackling bullying and how this relates to incidents of cyber-bullying

- To be mindful of protecting data and keeping access to digital information secure by adhering to the school password policy and protecting their accounts from student access.
- To use secure portable data options including password protected or encrypted portable memory devices

5.0 E-SAFETY IN THE CURRICULUM

5.1 E-safety is embedded into the curriculum at all age ranges. Lessons should be well planned and resourced and there should be a number of opportunities to discuss a range of e-safety issues.

5.2 E-safety is covered within ICT and PSHE lessons but is not exclusive to these subject areas and discussion of e-safety is explored in other subject areas both while using technology and as a topic as appropriate, including assemblies

5.3 Guidance on minimum coverage in each key stage:-

Communication and Language – pupils aware that they are able to communicate with others using devices – appropriate language and key words associated with technology

Physical development – safe and careful handling of technology

Personal, Social and Emotional development – sharing and cooperating while using technology

Understanding of the World – awareness of devices around us and how they are used to keep us safe, provide us with information

Pupils should be made aware of distinction between personal, private and public information. Pupils should be taught appropriate ways to communicate when using devices and how to respond to unpleasant or distressing comments they may encounter online. They should be made aware that people they do not know are strangers including while playing online games and the importance of using 'usernames' and guarding against volunteering information. They should be taught how to respond if they are distressed or uncertain about any material they are exposed to while online or

using technology.

Importance of passwords and cyber security. Understanding of how cyberbullying is using technology to be unpleasant and guidance on how to respond constructively and report any thing that concerns them. Understanding of how social networks allow sharing of information and the importance of keeping information about themselves private. Understanding of how data submitted to the Internet including photographs, comments, emails etc. can be potentially accessed, altered and used by anyone. Clearer understanding of distinction between private and public information. Discussion of support networks and methods of reporting anything they are uncertain or concerned about. Understanding of spam, unsolicited and scam activity on the Internet and how accounts can be hacked or accessed by criminals.

Discussion of E-safety issues in the news and current affairs. Understanding of the law and relevant acts passed to protect people from discrimination, abuse and exposure to indecent content. Discussion of how photographs, information and comments posted online can be accessed by any one and cannot be retracted or removed easily. Fuller understanding of how everyday use of technology can be made more secure through intelligent password use, vigilance and due care when using public technology facilities. Understanding of plagiarism and copyright laws. Addictive nature of devices. Access to relevant support networks and guidance on dealing with cyberbullying, peer pressure and social aspects of device use.

5.4 Extra –curricular activities such as Safer Internet Day opportunities, visits from local PSCO, school assemblies should be explored but these should not represent the majority of E-safety teaching or discussion in the academic year. They should be used to support lessons embedded in the curriculum.

5.5 Use of mobile devices during lessons is subject to control and risk management. Expectations of appropriate use of mobile devices are set out in the Pupil Planner for students. This includes students are expected not to share digital images or videos of other students taken during lessons for any purpose other than school use.

5.5 Opportunities for peer mentoring or 'buddy' systems can be explored so that older

pupils can act as role models for younger children and provide a further method for students to report concerns

5.6 Letters home to parents updating them with advice and information regarding E-safety. Talks from experts (both internal and external) to provide guidance on E-safety to both pupils and parents, including the Police.

6.0 INFRASTRUCTURE AND DATA MANAGEMENT

6.1 The school Internet access is subject to filtering and control and this is updated regularly

6.2 Staff are aware of how to use safe-searching options and are vigilant during lessons involving Internet access

6.3 Where available, screen watching facilities are used and staff are aware of how to utilise these resources

6.4 Passwords and digital security is in place to protect data and data is managed in accordance with the relevant DP Acts

6.5 Staff are fully aware of how to report a problem or any incidents relating to data security or Internet control

6.6 Professional communications between the school and other organisations or parents take place within clear professional boundaries, are transparent and open to scrutiny and do not share personal information with students

7.0 MONITORING, AUDIT AND POLICY REVIEW

7.1 The E-safety policy is dated and an annual review date is stated with a named member of staff responsible for ensuring it is reviewed and updated

7.2 It may be necessary for more frequent reviews if a number of incidents are recorded.

7.3 The review procedure should be:

- An audit of effectiveness of current practice
- A review of guidance published by relevant organisations

- Amendments to be shared with all staff

7.4 To audit E-safety effectiveness of the current policy the following questions should be   considered:

- Has recording of E-safety incidents been effective – are records kept?
- Did the school feel able to respond effectively to any incidents?
- Were incidents resolved to the best of the school's ability?
- Do all students demonstrate an awareness of E-safety appropriate to their age?
- Have complaints or concerns with the policy been recorded and addressed?
- Have there been significant developments in technology that should be addressed either within the curriculum or as part of staff awareness training?
- Is the policy clear to all staff and seen as appropriate and working?
- Is the current wording fit for purpose and reflective of technology use in the school?
- Do all members of the school community know how to report a problem?
- Is E-safety observed in teaching and present in curriculum planning documents?

See also:

- Any review notes from E-safety audits
- School mobile phone policy
- Agreed sanctions and rewards related to E-safety
- Lists of useful organisations and contacts for reporting safeguarding concerns
- School website policy

Signed:

Georgina Masefield, Head Teacher