ONLINE /
E SAFETY POLICY

Reviewed: October 2024
Next Review: October 2025

E Safety Policy Summary

E-Safety Policy – a summary

As an online learning provider, Apricot Online takes incredibly seriously its responsibility forseeking to secure and to promote E-Safety, for students, families and its own personnel.

This policy outlines the key responsibilities all personnel have within Apricot Online regarding E- Safety. It also outlines the strong accent we place on education for students, but also families andstaff about the key issues regarding E-Safety and how to identify and mitigate the risks.

The requirement to ensure that children and young people can use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work at Apricot Online are bound. The use of these exciting and innovativetools in school and at home has been shown to raise educational standards and promote Student achievement. However, the use of these new technologies, including the use of social media, can put young people at risk within and outside the school. Many of these risks reflect situations in the off-line world.

The policy details our arrangements for filtering and monitoring, as well our policies on the use ofdigital photographs and video and in relation to the use of social media, both by students and by staff. There are a number of key web-links to further advice and guidance, given the importance of disseminating the key learning about E-Safety to all within our community. The policy details how we will respond to instances of incidents involving social media and our communications approach.

This policy must be read in close conjunction with our **child protection and safeguarding** policy, inparticular:

- Section 7- recognising abuse and taking action (including ‘peer-on-peer’ abuse and sexting)
- Section 12- mobile phones and cameras
- Appendix 1 – types of abuse
- Appendix 3- specific safeguarding issues (including child criminal exploitation and childsexual exploitation and preventing radicalisation)

This policy should also be read in close conjunction with our **behaviour and attendance policy**, inparticular:

- Section 8- Anti-Bullying policy

1.Rationale

The requirement to ensure that children and young people can use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of careto which all who work at Apricot Online are bound. The use of these exciting and innovative tools inschool and at home has been shown to raise educational standards and promote Student achievement.

However, the use of these new technologies, including the use of social media, can put young peopleat risk within and outside the school. Many of these risks reflect situations in the off-line world and itis essential that this e-safety policy is used in conjunction with our **child protection and safeguarding policy.**

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential,through good educational provision to build Student ’ resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

As part of this policy, records will be maintained of E-Safety related incidents involving staff and Students and any incidents recorded will be treated in accordance with our safeguarding procedures.This policy will be reviewed at least annually.

The school will monitor the impact of the policy using: • Feedback from staff, Student, parents /carers, governors • Logs of reported incidents • Internet activity monitoring logs

2. **Scope of the Policy**

This policy applies to all members of the Apricot Online community who have access to and are users of our learning platforms.

3. **Roles and Responsibilities**

Apricot Board

The Apricot Board is responsible for the approval of the E-Safety Policy and for reviewing its effectiveness.

Operations Director

The Operations Director is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Designated Safeguarding Lead. The Operations Director is responsible for the implementation and effectiveness of this policy. They are also responsible for reporting to the Board on the effectiveness of the policy and, if necessary, for making any necessary recommendations re further improvement. The Operations Director is responsible for ensuring staff receive suitable CPD to enable them to carry out their e-safety roles. The Operations Director, Managing Director and Heads of Faculty will ensure that there is a system in place to allow for monitoring and support of those at Apricot Online who carry out the internal e-safety monitoring role. This is to provide a safety net and to support those colleagues who take on important monitoring roles. The Operations Director and Senior EducationTeam should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (See Managing Allegations against a member of staff – Apricot Online, Safeguarding policy)

The Designated Safeguarding Lead: takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing our e-safety policies / documents. she ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident takingplace. She reports to the Board serious breaches of the E-Safety Policies and provides training and advice for staff. She liaises with the Local Authority (where relevant) and receives reports of e-safety incidents. She creates a log of incidents to inform future e-safety developments. The DSL is trained in and shares with staff an awareness and understanding of e- safety issues and the potential for serious child protection issues that can arise from: Sharing of personal data, Access to illegal / inappropriate materials, Inappropriate on-line contact with adults / strangers, Potential or actual incidents of grooming, Cyber-bullying , Sexting, Revenge pornography, Radicalisation (extreme views), CSE.

(Senior) Leaders of Learning are responsible for ensuring that: they have an up to date awareness ofe-safety matters and of the current e-safety policy and practices. They should have read, understoodand signed the E–Safety policy and should report any suspected misuse or problem to the Designated Safeguarding Lead for investigation / action / sanction. Digital communications with students and parents / carers (email / voice) should be on a professional level.

Students understand and follow, as appropriate for age and ability, the e-safety policy. Students understand and follow e-safety rules and they know that if these are not adhered to, sanctions will be implemented in line with our behaviour and anti-bullying policies. In online lessons where internet use is planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. They need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so, where appropriate for age and ability. They are expected to follow school rules relating to this policy e.g. safe use of cameras, cyber-bullying etc. They should understand that the E-Safety Policy covers their actions out of school, if related to theirmembership of Apricot Online, where appropriate for age and ability.

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of technology than their children.
Apricot Online will therefore take every opportunity to help parents understand these issues through parents’ evenings, letters, website / local e-safety campaigns / literature.

4. **Education and Training**

Education – Students

E-Safety education will be provided in the following ways, as appropriate to a students’ age and ability: A planned e-safety programme will be provided as part of Computing / PHSE / other lessons and should be regularly revisited – this will cover both the use of new technologies in school and outside school.
Students should be encouraged to adopt safe and responsible use of technology, the internet and mobile devices both within and outside school. They should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. They are taught the importance of keeping information such as their passwords safe and secure. Rules for the use of systems / internet will be made available for students to read. Staff should act as good role models in their use of learning

platforms, the internet and mobile devices. Studentsare taught how to keep safe though effective / good e-safety practice as part of an integral element of the school Computing curriculum and within their own learning. They are allowed to freely search the internet, e.g., using search engines. Staff should be vigilant in monitoring the content of the websites the young people visit. It is accepted that from time to time, for good educational reasons,students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT team can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents and Carers

Some parents and carers will have only a limited understanding of e-safety risks and issues, yet theyplay an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents may either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

We will therefore seek to provide information and awareness to parents and carers through: Letters,our web sites, parents evenings, reference to external e-safety websites, high profile events such as Internet safety day and family learning opportunities.

Education & Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, asoutlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This willbe regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand Apricot Online online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Online Safety Lead will provide advice/guidance/training to individuals as required.

5. Technical – Infrastructure / equipment, filtering and monitoring

Apricot will be responsible for ensuring that its infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It has detailed procedures in place for this to happen. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities. School systems will be managed through the managed service provider. All users will have clearly defined access rights to school systems. Staff will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Appropriate security measures are in place, provided by the managed service provider, to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure is protected by up to date antivirus software. Personal data cannot be sentover the internet or taken off the system sites unless safely encrypted or otherwise secured in accordance with the school Personal Data Policy.

6. Use of digital photographs and video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and Students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and Studentsneed to be aware of the risks associated withsharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. We will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

Staff are allowed to take digital / video images to support educational aims, but must follow guidance here concerning the storing, sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes. Care should be taken when taking digital / video images that Students are appropriately dressed and are not participating in activities that might bring the individuals or Apricot Online into disrepute. Students must not take, use, share, publish or distribute images of others without their permission.

Written permission from parents or carers will be obtained before photographs of students/Student together with their name are displayed on school displays, in newsletters and in their child’s own and other children’s learning workbooks. Written permission from parents or carers will be obtainedbefore photographs of students together with their name displayed alongside are published in leaflets, posters, documents, training materials or used by the press.

Written permission from parents or carers will be obtained before photographs of students/Students are published on Apricot Online’s websites or social media. Students full names will not be used anywhere on a website or blog, particularly in association with photographs. Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

7. Use of social media sites by students

The use of new technologies, including the use of social media, can put young people at risk withinand outside the school. Some of the dangers they may face include: access to illegal, harmful or inappropriate images or other content un-authorised access to / loss of / sharing of personal information, the risk of being subject to grooming by those with whom they make contact on a socialmedia platform, the sharing / distribution of personal images without an individual's consent or knowledge, inappropriate communication / contact with others, including strangers, cyber-bullying, the potential for excessive use which may impact on the social and emotional development and learning of the young person.

Apricot Online is committed to supporting parents and students in raising awareness of the issues involved in using social networking sites for young people, including:

Content: children who create or post inappropriate, offensive or even illegal content in their own orothers' pages and feeds could get themselves into trouble with their school, friends, or even break the law, depending on the nature of the material. It is also important that young people understandthe longevity of posting something online.

Contact: many young people need to be aware that any personal information they upload could potentially reach a much wider audience than intended. If a user of a social networking service doesnot protect their information by enabling the correct privacy settings, they could be exposing their information to strangers and as a result be at risk of online contact and grooming. Posting or chatting about personal details might enable someone to identify and contact a child online or in person. There is also the more likely risk of cyberbullying with young people intentionally harming another person online.

Privacy settings: these settings give the user the ability to control who they share particular contentwith, for example making a photo to post visible to friends only or to the public. We will encourage children and young people to use the privacy tools available on the social networking service to protect their personal information and to keep their passwords private (even from their friends).

Online Friendship: the importance of children considering carefully who they add as friends or followers, and what those friends and followers can see once added to a contact list. Their mosttrustworthy online friends are the people you also know and trust offline.

Geolocation; young people must be aware of who they are sharing their location with. If they are accessing a social networking services via a smartphone or mobile device, they might be disclosingtheir location without realising it. Location services can be turned on or off per app within the settings of a device.

Think Before You Post; the importance of thinking before you post something online. This can include writing a comment or sharing a picture. It can also include sharing on things that others haveposted. What may start out as a harmless joke for one person can be extremely hurtful for another individual and once something is posted online it is potentially there forever.

Consider the photos you upload; that children consider the content of the images they share online,and the impact they may have on their own reputation, and the emotions of others. They should always ensure that they ask permission from others before posting pictures of them online.

Know how to block and report; that children know how to report abusive comments or illegal activity on social networking services. Many social networking sites allow you to report a commentor user who is potentially breaking their terms and conditions, by clicking on a report button or filling out an online form. If young people have concerns about cyber-bullying then they should speak to a trusted adult as well as save the evidence and use the tools available to block other users.

Security; making sure children choose a strong password and that they have locked their mobiledevice with a pin or password, as mislaid devices can mean that others could access their social networking accounts.

Leaders and teachers at Apricot Online will actively refer parents to guidance at sites such as:

Childnet International – Young people and social networking services

The UK Council for Child Internet Safety (UKCCIS)-Child Safety Online- a practical guide

NSPCC: Child safety online: a practical guide for parents and carers whose children are using socialmedia

8. Use of social media by Apricot Online personnel

The purpose of this advice note is to guide the judgements of management and staff using social networking sites and the information that they provide through these by:

a. advising management and staff to ensure that children are safeguarded
b. advising management and staff to ensure that the reputation of the school is not adversely affected through use of social networking sites.
c. ensuring that the school is not subject to legal challenge as a result of school employee susing and providing information on social networking sites e.g. data protection, discrimination and other sensitive information.

Leaders should make all staff aware of this advice note and the expectations of staff conduct related to social networking. For new staff this should form part of their induction.

Social networking applications include, but are not limited to: Blogs, Online discussion forums, Collaborative spaces, Media sharing services, 'Microblogging' applications. Examples include Twitter, Facebook, MSN, You Tube, Yammer.

9. Apricot Online Staff Code of Conduct

(Please see full Staff Code of Conduct policy)
In general terms, Apricot Online expects that the conduct of its employees is such that no justifiable complaint can be made by parents, Student , colleagues, Academic Council members, other bodies or agencies or members of the community in relation to conduct and behaviour of school staff. Thisprinciple applies to the use of social networking sites.

The way in which school staff present and conduct themselves on social networking sites can havean impact on the public perception of the school and influence the way in which those staff members are perceived by Students and parents of the school. In their use of social networking sites,staff should be aware that that their online behaviour could affect their professional standing, dignity and perception of their integrity.

It is recommended that school staff take adequate precautions when using social networking sites/applications, both in vetting material that could be connected to them (through their own profile and information added about them) and through the use of appropriate security settings.

School employees should not be “friends” with Students on social networking sites as this would be viewed as a safeguarding issue. It is recommended that the school seeks advice from the Designated Safeguarding Lead on their personal use of social networking sites and/or report concerns about the inappropriate use of a social networking site/application by another member of staff. Where Students behave inappropriately with staff this should be reported to a member of the senior leadership teamand dealt with through the Student disciplinary process.

Conduct by staff that is a gross misconduct – e.g. entering into a personal relationship with a Student : criminal offences and other conduct outside employment could cause an employee’s position at theschool to become untenable, particularly in circumstances where the conduct or offence is unacceptable to colleagues, management or parents or where the conduct or offence has the potential to affect the reputation of the school. This includes the making defamatory statements in the course of employment (e.g. making statements that are or could be slanderous or libellous) whether orally, written, or in electronic communication.

Breaches of these disciplinary rules in relation to social networking or any inappropriate use of socialnetworking sites and applications by staff will be dealt with through the School’s Disciplinary Procedure.

10. Dealing with social media ‘incidents’

A breach of the ‘social media use’ policy predisposes that there is a standard (often discretionary) below which an ‘incident’ has happened. In short, the standard must make it clear that all members of the school community must not post or share content that is threatening, hurtful or defamatory. Additionally, the sending by students of abusive or inappropriate messages or content via mobile phones or personal devices would amount to a breach of the school’s policy on behaviour. Offensiveor derogatory content stored on the same devices would also amount to a breach of the school’s policy.

Concerns relating to the online conduct of any member of the school community should be reportedto the DSL, especially if the concerns raised are safeguarding-related. The DSL, in turn, will determine, after an assessment of the information presented to them, whether to refer the matter onto the relevant local authority’s designated officer (LADO).

We, usually the DSL, will contact the police and inform the LADO if we believe a member of staff hascommitted a criminal offence using a personal device or mobile phone.

If aware of malicious online activity, we will take several sequential steps:
We will report malicious activity and seek support from an appropriate lead or manager and take screenshots of the offending content or web pages and record the time and date. Mediation or disciplinary procedures can be applied if the offender is a Student or colleague. If the offender is an adult, they should be invited to a meeting with a senior member of staff to address the concerns. If those responsible for offensive or inappropriate online content are known, the school should ensurethey understand why the material is unacceptable and request that they remove it. If the person refuses to remove the material, either report the matter to the social networking site or seek advice-agencies such as the UK Safer Internet Centre can also provide advice (web details above). Online harassment may amount to criminal conduct. If the material is of a sexual nature, sexist, threatening, abusive or constitutes a hate crime, consideration should be given to contacting the police. Employers have a duty of care to staff, and no-one should feel victimised in the workplace; support can be sought from the senior management team, HR

and union representatives if appropriate.

The UK Safer Internet Centre, which has developed strategic partnerships with internet industry key players, offers a free service for those working with children and young people: The Professional Online Safety Helpline provides advice, mediation and signposting to resolve e-safety issues with thesafety and policy teams at Rate My Teacher, Ask.FM, Google, Facebook, Twitter, YouTube, Tumblr and others. Facebook has launched the Bullying Prevention Hub and produced a support sheet specifically for teachers called ‘empower educators’.

11. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. More detailed guidance on the collection, handling and storage of personal data can be found in the Apricot Online Data Protection Policy.

12. Communications

When using communication technologies, Apricot Online considers the following as good practice. The official email service may be regarded as safe and secure.Users need to be aware that email communications may be monitored. Users must immediately report to the Designated Safeguarding Lead – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email. Any digital communication between staff and students or parents / carers must be professional in tone and content and be via official used systems.

Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusivematerial. Personal information should not be placed on the school website on public facing calendars and only official school emails should be identified within it. The school allows staff to bring in their own personal devices, including mobile phones, for their own use.

13. Responding to incidents of misuse

There may be times when infringements of the policy could take place, through careless or irresponsible actions or, very rarely, through deliberate misuse. Apricot Online has comprehensive procedures in place to deal with any incidents. If any apparent or actual misuse by Student , staff or any other user appears to involve illegal activity i.e. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material, other criminal conduct,activity or materials, the incident will be treated in accordance with the safeguarding policy and if necessary, the police would be informed. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner.

14. Monitoring and review

This policy will be reviewed annually, or earlier, if necessary, in line with national and/or local updates.