SPARSHOLT
COLLEGE HAMPSHIRE

ANDOVER COLLEGE
prepared for life

e-Safety Policy

Integrity, Valuing Others

Principal: Tim Jackson BTech (Hons), PGCE

Our Vision Statement

To inspire learners to recognise and achieve their full potential

Our Mission Statement

Excellence, Passion, Team Work, Integrity, Innovation,

Sustainability, Valuing Others and Supportiveness

Sparsholt College Hampshire, incorporating Andover College Hampshire

The *e-Safety Policy* was reviewed and reconfirmed by the Board of Governors in March 2018.

Equality Impact Assessment	Conducted: December 2011
Originator: Learning Technology Manager	Located: College Intranet
Date of next review: January 2021	

e-Safety Policy

Integrity, Valuing Others

Contents

e-Safety Policy

Integrity, Valuing Others

1. Policy Statement

Sparsholt College Hampshire ("the College") recognises the benefits and opportunities which new technologies offer to teaching and learning. We encourage the use of technology in order to enhance skills and promote achievement. However, the accessible and global nature of the internet and variety of technologies available mean that we are also aware of potential risks and challenges associated with such use.

Our approach is to implement safeguards within the College and to support staff and learners (i.e. students) to identify and manage risks independently. The College believes this can be achieved through a combination of security measures, training and guidance and implementation of our associated policies. In continuing our duty to safeguard learners, the College will do all that it can to make learners and staff stay e-safe and to satisfy its wider duty of care.

This e-Safety Policy should be read in conjunction with other relevant College policies: Safeguarding, Acceptable Use, Text Messaging, Learner Conduct & Performance, Staff Code of Conduct and Disciplinary.

2. Policy Scope

The policy applies to all members of the College community who have access to the College's IT systems, both on the premises and remotely. Any user of College IT systems must adhere to the Acceptable Use Agreement. The e-Safety Policy applies to all use of the internet and electronic communication devices such as email, mobile and smart phones, games consoles, social networking sites etc.

3. Roles and Responsibilities

There are clear lines of responsibility for e-safety within the College, with e-safety being one of the areas covered by the College Safeguarding Group. The first point of contact should be the Head of Student Services. All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager. Teaching staff are required to inform learners about e-safety during their induction and to read through and adhere to the incident reporting identified in section 7. When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

All learners should be informed sufficiently to know what to do if they have e-safety concerns and who to talk to. In most cases, this would be their pastoral tutor or a member of Student Services. Where any report of an e-safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where management considers it appropriate, the Learner Protection Officer may be asked to intervene with appropriate additional support from external agencies.

a. Learners:

Learners are expected to use the College IT systems and mobile devices in accordance with the College's Acceptable Use Policy, which they must agree to. Learners have an IT induction which will include e-safety guidance. They are expected to seek help and follow procedures where they are worried or concerned, or where they believe an e-safety incident has taken place involving them or another member of the College community. Learners are also required to act safely and responsibly at all times when using the internet and/or mobile technologies.

b. Staff:

All staff are required to use the College IT systems and mobile devices in accordance with the College's Acceptable Use Policy which they must actively promote through embedded good practice. Staff are required to attend relevant training sessions and to act as a model example to learners at all times.

All digital communications with learners should be professional in tone and content at all times. Online communication with learners must only be done through the College's network and the VLE. In the event of the need for the use of social networking sites, this should only occur with prior authority from line managers for specific uses, which will largely be connected to marketing activity or group communication. For more details please see the Social Networking Policy.

All staff should apply relevant College policies and understand the incident reporting procedures. Any incident that is reported to or discovered by a staff member must be reported to their line manager without delay.

4. Behaviour

All users of technologies should adhere to the standard of behaviour as set out in the Acceptable Use Policy. The College cannot and will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and learners should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated as a very serious matter in line with the Learner Conduct and Performance Policies and staff Disciplinary Policy. Where conduct is found to be unacceptable, the College will deal with the matter internally. Where conduct is considered illegal, the College will report the matter to the police.

5. Security

The College will do all that it can to make sure the College systems are safe and secure. Every effort will be made to keep security systems effective and up to date. Appropriate security measures will include the use of enhanced layer 2 filtering (iBoss), protection of firewalls, servers, routers and work stations etc. to prevent accidental or malicious access to college systems and information. All digital transactions on the College network, including email and internet postings, will be monitored by the IT Services team.

If wanting to make use of new technologies and online platforms, all staff must first discuss their requirements with either the ILT Strategic Advisory Group or the Safeguarding Group (Quality Improvement and Performance Manager or Head of Student Services).

6. Use of Images and Video

The use of images or photographs in teaching and learning is encouraged where there is no breach of copyright or other rights of another person. This will include images downloaded from the internet and images belonging to staff or learners.

Staff should make themselves aware of the risks in downloading these images as well as posting them online and sharing them with others. There are particular risks where personal images are posted onto social networking sites, see Social Networking Policy.

The College’s aim is to reinforce good practice as well as to offer further information for all users on how to keep their personal information safe.

No image/photograph of students can be copied, downloaded, shared or distributed online without permission. Photographs of activities on the College premises should be considered carefully before being published.

7. Incidents and Response

Where an e-safety incident is reported to the College, this matter will be dealt with as urgent and important. The College will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to their tutor or to the Student Services helpdesk. Where a member of staff wishes to report an incident, they must contact their line manager. Following any incident, the College will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. This is in line with the College’s Acceptable Use Policy. Serious incidents will be dealt with by the Strategic Leadership Team, in consultation with appropriate external agencies.