CRESSEY COLLEGE

e-SAFETY POLICY

Date Issued: 17 Oct 2016	Last Revised: 01 Sept 2018
Uncontrolled copy when printed (may be out of date)	

Table of Contents

Amendment Record

This e-Safety policy is reviewed to ensure its continuing relevance to the direction and processes that it describes. A record of additions, admissions and amendments is given below:

Version	Amendments	Date
1	Annual update to Policy. Minor amendments to formatting and wording. Approved at Management meeting dated 17 Oct 16. Authorised by JH, approved by Headteacher - AB.	17 Oct 16
2	Update to password policy. Approved at Management meeting dated 11 Jan 17. Authorised by BU, approved by HeadTeacher – AB	12 Jan 17
3	Annual update to Policy. Approved at Management meeting dated 30 Aug 17. Authorised by BU, approved by Head Teacher – AC.	01 Sept 17
4	Annual update to Policy. Approved at Management meeting dated 29 Aug 18. Authorised by BU, approved by Head Teacher – AC.	01 Sept 18

Introduction and Overview

Rationale

1. The purpose of this policy is to:

   a. Set out the key principles expected of all members of the school community at Cressey College with respect to the use of ICT-based technologies.

   b. Safeguard and protect the children and staff of Cressey College.

   c. Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.

   d. Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.

   e. Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.

   f. Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

   g. Minimise the risk of misplaced or malicious allegations made against adults who work with students.

2. The main areas of risk for our school community can be summarised as follows:

   a. Content.

      1) Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.

      2) Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.

      3) Hate sites.

      4) Content validation: how to check authenticity and accuracy of online content.

   b. Contact.

      1) Grooming.

      2) Cyber-bullying in all forms.

      3) Identity theft (including ‘frape’ (hacking Facebook profiles)) and sharing passwords.

   c. Conduct.

      1) Privacy issues, including disclosure of personal information.

      2) Digital footprint and online reputation.

      3) Health and well-being (amount of time spent online (Internet or gaming)).

4) Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images).

5) Copyright (little care or consideration for intellectual property and ownership – such as music and film). (Ref Ofsted 2013).

Scope

3. This policy applies to all members of Cressey College community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of Cressey College.

4. The Education and Inspections Act 2006 empowers Head Teachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

5. The School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and key responsibilities

6. Headteacher.

a. To take overall responsibility for e-safety provision.

b. To take overall responsibility for data and data security.

c. To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements.

d. To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant.

e. To be aware of procedures to be followed in the event of a serious e-safety incident.

f. To receive regular monitoring reports from the E-Safety Co-ordinator (Sweethaven Education Services).

g. To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager).

7. E-Safety Co-ordinator / Designated Child Protection Lead.

a. Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.

b. Promotes an awareness and commitment to e-safeguarding throughout the school community.

c. Ensures that e-safety education is embedded across the curriculum.

d. Liaises with school ICT technical staff (Sweethaven).

e. To communicate regularly with SLT to discuss current issues, review incident logs and filtering / change control logs.

f. To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident.

g. To ensure that an e-safety incident log is kept up to date.

h. Facilitates training and advice for all staff.

i. Liaises with the Local Authority and relevant agencies.

j. Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:

1) Sharing of personal data.

2) Access to illegal / inappropriate materials.

3) Inappropriate on-line contact with adults / strangers.

4) Potential or actual incidents of grooming.

5) Cyber-bullying and use of social media.

8. Senior Leadership Team.

a. To ensure that the school follows all current e-safety advice to keep the children and staff safe.

b. To approve the E-Safety Policy and review the effectiveness of the policy.

c. Receive regular information about e-safety incidents and monitoring reports.

d. To support the school in encouraging parents and the wider community to become engaged in e-safety activities.

9. ICT Teaching Staff

a. To oversee the delivery of the e-safety element of the Computing curriculum.

b. To liaise with the e-safety coordinator/Heads of Department regularly.

10. Network Manager/technician (Sweethaven).

a. To report any e-safety related issues that arises, to the e-safety coordinator/Business & Contracts Manager.

b. To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed.

c. To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date).

d. To ensure the security of the school ICT system.

e. To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices.

f. The school's policy on web filtering is applied and updated on a regular basis.

g. That he / she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

h. That the use of the network / Office 365 / remote access / email is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Co-ordinator / Headteacher for investigation, action & sanction.

i. To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

j. To keep up-to-date documentation of the school's e-security and technical procedures.

11. Admin Team.

a. To ensure that all data held on students on SIMs is adequately protected.

b. To ensure that all data held on students on the school office machines have appropriate access controls in place.

12. Teachers.

a. To embed e-safety issues in all aspects of the curriculum and other school activities.

b. To supervise and guide students carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant).

c. To ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.

13. All staff are:

a. To read, understand and help promote the school's e-safety policies and guidance.

b. To read, understand, sign and adhere to the school staff Acceptable Use Agreement.

c. To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

d. To report any suspected misuse or problem to the e-safety coordinator / Head Teacher.

e. To maintain an awareness of current e-safety issues and guidance e.g. through CPD.

f. To model safe, responsible and professional behaviours in their own use of technology.

g. To ensure that any digital communications with students should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones, social media sites etc.

14. Students

a. Read, understand, sign and adhere to the Student Acceptable Use Policy (NB: at KS1 it would be expected that parents / carers would sign on behalf of the students).

b. Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

c. To understand the importance of reporting abuse, misuse or access to inappropriate materials.

d. To know what action to take if they or someone they know feels worried or vulnerable when using online technology.

e. To know and understand school policy on the use of mobile phones, digital cameras and hand held devices.

f. To know and understand school policy on the taking / use of images and on cyber-bullying.

g. To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

h. To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home.

i. To help the school in the creation/ review of e-safety policies.

15. Head Teacher & Police Liaison Officers.

    a. Educating Parents and raising awareness.

16. Parents/carers.

    a. To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the students' use of the Internet and the school's use of photographic and video images.

    b. To read, understand and promote the school Student Acceptable Use Agreement with their children.

    c. To consult with the school if they have any concerns about their children's use of technology.

17. External groups.

    a. Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school.

Communication:

18. The policy will be communicated to staff/students/wider community in the following ways:

    a. Policy to be posted on the school website & Office 365.

    b. Policy to be part of school induction pack for new staff.

    c. Acceptable use agreements discussed with students at the start of each year.

d. Acceptable use agreements to be issued to whole school community, usually on entry to the school.

e. Acceptable use agreements to be held in student and personnel files.

Handling complaints:

19. The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

20. Staff and students are given information about infringements in use and possible sanctions. Sanctions available include:

a. Interview/counselling by tutor / senior teacher / E-Safety Coordinator / Headteacher.

b. Informing parents or carers.

c. Removal of Internet or computer access for a period, (which could ultimately prevent access to files held on the system, including examination coursework).

d. Referral to LA / Police.

21. Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

22. Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school Safeguarding Policy / LA child protection procedures.

Review and Monitoring

23. The e-safety policy is referenced from within other school policies: ICT and Computing policy, Safeguarding policy, Anti-Bullying policy, in the School Development Plan, Behaviour policy, Personal, Social and Health Education policies.

24. The school has an e-safety coordinator (senior teacher on each site) who will be responsible for document ownership, review and updates.

25. The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.

26. The e-safety policy has been written by the Head Teacher and is current and appropriate for its intended audience and purpose.

27. There is widespread ownership of the policy and it has been agreed by the SLT. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

Education and Curriculum

Student e-safety curriculum

28. This school:

a. Has a clear, progressive e-safety education programme as part of the ICT/Computing curriculum / PSHE curriculum. It is built on LA/DFE e-safeguarding and e-literacy framework national guidance. This covers a range of skills and behaviours appropriate to the students age and experience, including:

1) To STOP and THINK before they CLICK.

2) To develop a range of strategies to evaluate and verify information before accepting its accuracy.

3) To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be.

4) To know how to narrow down or refine a search.

5) For older students: to understand how search engines work and to understand that this affects the results they see at the top of the listings.

6) To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.

7) To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.

8) To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments.

9) To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.

10) To understand why they must not post pictures or videos of others without their permission.

11) To know not to download any files – such as music files - without permission.

12) To have strategies for dealing with receipt of inappropriate materials.

13) For older students; to understand why and how some people will 'groom' young people for sexual reasons.

14) To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.

15) To know how to report any abuse, including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK STOP button.

b. Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

c. Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school.

d. Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.

e. Ensures that when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights.

f. Ensures that staff and students understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include: risks in pop-ups; buying on-line; on-line gaming and gambling.

Staff training

29. This school:

a. Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.

b. Makes regular training available to staff on e-safety issues and the school's e-safety education programme: all staff undertake e-safety e-learning modules as part of their induction.

c. Provides, as part of the induction process, all new staff (including those on university/college placement and work experience) with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

30. This school:

a. Will introduce a programme of advice, guidance and training for parents, including:

1) Introduction of the Acceptable Use Agreements to parents, to ensure that principles of e-safe behaviour are made clear.

2) Information leaflets; in school newsletters and on the school web site.

3) Demonstrations, practical sessions held at school.

4) Suggestions for safe Internet use at home.

5) Provision of information about national support sites for parents.

Expected Conduct and Incident management

Expected conduct

31. In this school, all users:

a. Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (at KS1 it would be expected that parents/carers would sign on behalf of the students).

b. Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.

c. Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

d. Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

e. Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

Staff

32. Are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students/Students

33. Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers

34. Should provide consent for students to use the Internet, as well as other technologies, as part of the e-safety Acceptable Use Agreement form at time of their child's entry to the school

35. Should know and understand what the 'rules of appropriate use' are and what sanctions could result from misuse.

Incident Management

36. In this school:

a. There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though if the attitudes and behaviour of users are generally positive there is rarely need to apply sanctions.

b. All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.

c. Support is actively sought from other agencies as needed (e.g. the local authority, Sweethaven Education Services, UK Safer Internet Centre helpline) in dealing with e-safety issues.

d. Monitoring and reporting of e-safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders.

e. Parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.

f. We will contact the Police if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law.

Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

37. This school:

a. Uses filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students.

b. Ensures network health through use of Sweethaven managed anti-virus software and network set-up so staff and students cannot download executable files.

c. Uses approved systems such as secured email to send personal data over the Internet or uses encrypted devices.

d. Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Office 365 system.

e. Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons.

f. Has blocked student access to music download or shopping sites – except those approved for educational purposes at a regional or national level.

g. Uses security time-outs on Internet access where practicable / useful.

h. Works to ensure any concerns about the system are communicated so that systems remain robust and protect students.

i. Is vigilant in its supervision of students' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older students have more flexible access.

j. Ensures all staff and students have signed an Acceptable Use Agreement form and understands that they must report any concerns.

k. Ensures students only publish within an appropriately secure environment.

l. Requires staff to preview websites before use (where not previously viewed or cached).

m. Plans the curriculum context for Internet use to match students' ability, using child-friendly search engines, where more open Internet searching is required; e.g. yahoo for kids or ask for kids and Google Safe Search.

n. Never allows / is vigilant when conducting 'raw' image search with students e.g. Google image search.

o. Informs all users that Internet use is monitored.

p. Informs staff and students that that they must report any failure of the filtering systems. Our system administrator(s) logs or escalates as appropriate any reported failures to the Technical service provider (Sweethaven Education Services) as necessary.

q. Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions could result from misuse – through staff meetings and teaching programme.

r. Provides advice and information on reporting offensive materials, abuse/ bullying etc is available for students, staff and parents.

s. Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Network management (user access, backup)

38. This school:

a. Uses individual, audited log-ins for all users.

b. Ensures the Systems Administrator / network manager is up-to-date with policies / requires the Technical Support Provider to be up-to-date with services and policies.

c. Storage of all data within the school will conform to the UK Data Protection requirements.

d. Students and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

39. To ensure the network is used safely, this school:

a. Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password.

b. Staff access to the Schools' Management Information System is controlled through a separate password for data security purposes.

c. We will provide students with an individual network log-in username. From Year 7 they are also expected to use a personal password.

d. All students have their own unique username and password which gives them access to the Internet.

e. Makes clear that no one should log on as another user and makes clear that students should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network.

f. Has set-up the network with a shared work area for students and one for staff. Staff and students are shown how to save work and access work from these areas.

g. Requires all users to always log off when they have finished working or are leaving the computer unattended.

h. Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.

i. Requests that teachers and students do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day.

j. Has set-up the network so that users cannot download executable files / programmes.

k. Has blocked access to music/media download or shopping sites – except those approved for educational purposes.

l. Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus software maintained up-to-date.

m. Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.

n. Maintains equipment to ensure Health and Safety is followed.

o. Has integrated curriculum and administration networks, but access to the Schools' Management Information System is set-up so as to ensure staff users can only access modules related to their role, e.g. teachers access report writing module; SEN coordinator - SEN data.

p. Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems.

q. Does not allow any outside Agencies to access our network remotely, except where there is a clear professional need and then access is restricted and is only through approved systems, e.g. technical support or SMIS Support; accessing attendance data on specific children, parents using a secure portal to access information on their child.

r. Provides students and staff with access to content and resources, which staff and students access using their username and password.

s. Makes clear responsibilities for the daily back up of SMIS and finance systems and other important files.

t. Uses the DFE secure s2s website for all CTF files sent to other schools.

u. Where practicable, ensures that all student level data or personal data sent over the Internet is encrypted or only sent within the approved secure system.

v. Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network.

w. Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use.

x. All computer equipment is installed professionally and meets health and safety standards.

y. Projectors are maintained so that the quality of presentation remains high.

z. Reviews the school ICT systems regularly with regard to health and safety and security.

Password policy

40. This school makes it clear that staff and students must always keep their password private, must not share it with others and must not leave it where others can find it (this includes computer, work e-mail & Office 365 access passwords).

41. All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

42. We require staff to use STRONG passwords for access into all our IT systems (a mixture of upper & lower case and numbers).

43. We require staff to change their passwords into the Office 365 system twice a year.

E-mail

44. This school:

a. Provides staff with an email account for their professional use, through Office 365, and makes clear personal email should be through a separate account.

b. Does not publish personal e-mail addresses of students or staff on the school website. We use anonymous or group e-mail addresses, for example info@cresseycollege.co.uk for communication with the wider public.

c. Will contact the Police if one of our staff or students receives an e-mail that we consider is particularly disturbing or breaks the law.

d. Will ensure that e-mail accounts are maintained and up to date.

e. Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.

f. Knows that spam, phishing and virus attachments can make e-mails dangerous. We use a number of provided technologies to help protect users and systems in the school, including desktop anti-virus plus appropriate website filtering for schools.

Students:

45. Students are introduced to, and use e-mail as part of the ICT/Computing Scheme of Learning.

46. Students can only receive external mail from, and send external mail to, addresses if the SafeMail rules have been set to allow this.

47. Students are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:

a. Not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer.

b. That an e-mail is a form of publishing where the message should be clear, short and concise.

c. That any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

d. They must not reveal private details of themselves or others in email, such as address, telephone number, etc.

e. To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe.

f. That they should think carefully before sending any attachments.

g. Embedding adverts is not allowed.

h. That they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature.

i. Not to respond to malicious or threatening messages.

j. Not to delete malicious or threatening e-mails, but to keep them as evidence of bullying.

k. Not to arrange to meet anyone they meet through e-mail, without having discussed with an adult and taking a responsible adult with them.

l. That forwarding 'chain' e-mail letters is not permitted.

m. Students sign the school Acceptable Use Agreement form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff

48. Staff can only use the Office 365 e-mail systems on the school system.

49. Staff only use Office 365 e-mail systems for professional purposes.

50. Access in school to external personal e-mail accounts may be blocked.

51. Always use secure e-mail or password protection to transfer staff or student personal data.

52. Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':

a. The sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used.

b. The sending of chain letters is not permitted.

c. Embedding adverts is not allowed.

d. All staff sign our school Acceptable Use Agreement form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School website

53. The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained. In addition:

a. Only authorised users may upload information to the school's website.

b. The school web site complies with the statutory DFE guidelines for publications.

c. Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.

d. The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. info@schooladdress or admin@schooladdress. Home information or individual e-mail identities will not be published, or kept to an absolute minimum.

e. Photographs published on the web do not have full names attached.

f. We do not use students' names when saving images in the file names or in the tags when publishing to the school website.

g. We do not use embedded Geodata in respect of stored images.

Office 365

54. Uploading of information on the schools' Office 365 space is shared between different staff members according to their responsibilities.

55. Photographs and videos uploaded to the schools Office 365 will only be accessible by members of the school community.

Social networking

56. Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students.

57. School staff will ensure that in private use:

a. No reference should be made in social media to students, parents / carers or school staff.

b. They do not engage in online discussion on personal matters relating to members of the school community.

c. Personal opinions should not be attributed to Cressey College or local authority.

d. Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing

58. This school only uses approved or checked webcam sites.

CCTV

59. We currently do not have CCTV installed at any of Cressey College school sites.

Data security: Management Information System access and data transfer

Strategic and operational practices

60. At this school:

a. The Head Teacher is the Senior Information Risk Officer (SIRO).

b. Staff are clear who the key contact(s) for key school information are.

c. We ensure staff know to report any incidents where data protection may have been compromised and to whom.

d. All staff are DBS checked and records are held in one central record.

e. We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed:

1) Staff.

2) Students.

3) Parents.

f. This makes clear staff responsibilities with regard to data security, passwords and access.

61. We follow LA guidelines for the transfer of any data, such as SIMS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.

62. No Protected and Restricted material must be removed from the school without the permission of the HeadTeacher.

63. School staff with access to setting-up usernames and passwords for email, network access and Office 365 access are working within the approved system and follow the security processes required by those systems.

64. We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

65. Staff have secure area(s) on the Office 365 network to store sensitive documents or photographs – this must always be authorised through the School Office Manager.

66. We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.

67. We use the DFE S2S site to securely transfer CTF student data files to other schools.

68. We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.

69. All servers are in lockable locations and managed by DBS-checked staff.

70. Paper based sensitive information is shredded, using a cross cut shredder.

Equipment and Digital Content

Personal mobile phones and mobile devices

71. Mobile phones brought into school are entirely at the staff member, student & parent or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.

72. Student mobile phones which are brought into school must be turned off and handed in to school staff to store safely on arrival at school. Staff members may use their phones during school break times. All visitors are requested to keep their phones on silent. Students will be given their phones back at the end of the school day.

73. The recording, taking and sharing of images, video and audio on any mobile phone is not permitted. All mobile phone use is to be open to scrutiny and the Head teacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

74. The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.

75. Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

76. Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.

77. Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

78. Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.

79. Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a senior member of staff.

80. The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.

81. No images or videos should be taken on mobile phones or personally-owned mobile devices.

82. All mobile phones and personally-owned devices will be handed in at the respective School office should they be brought into school.

Students' use of personal devices

83. The School strongly advises that student mobile phones should not be brought into school.

84. The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.

85. All students are required to hand their phone in to school staff on arrival to school. There are no exceptions to this rule.

86. If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.

87. Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

88. If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

89. Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences. Students will be provided with school mobile phones to use in specific learning activities under the supervision of

a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.

Staff use of personal devices

90. Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

91. Staff will be issued with a school phone where, above normal contact with students, parents or carers is required.

92. Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

93. If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.

94. Staff must not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.

95. If a member of staff breaches the school policy then disciplinary action may be taken.

96. Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide their own mobile number for confidentiality purposes (by inputting 141 before they dial the number).

97. **Digital images and video**

98. In this school:

a. We gain parental / carer permission for use of digital photographs or video involving their child as part of the school consent forms when their daughter / son joins the school.

b. We do not identify students in online photographic materials or include the full names of students in the credits of any published school produced video materials / DVDs.

c. Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of students.

d. If specific student photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or student permission for its long term use.

e. The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.

f. Students are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include parents or younger children as part of their ICT scheme of learning.

g. Students are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

h. Students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

99. Details of all school-owned hardware will be recorded in a hardware inventory.

100. Details of all school-owned software will be recorded in a software inventory.

101. All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

102. All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.

103. Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.