CRANSLEY SCHOOL

E-Safety Policy

Seeking Excellence | Nurturing Relationships | Venturing Beyond

Reviewer	Status	Notes
JC	Approved	Changes regarding roles and responsibilities Highlights to network security, firewalls and net filters Highlighting teachers' roles in identifying unsafe practice highlighting the four C's of risk
JPG	Approved	Alignment with KCSIE 2022
RP	Approved	ADjustment and clarification
Governors	Approved	Reviewed by DW. Questions and Queries Board of Govs Meeting - 26 September 2022

Date for Review – September 2024

CRANSLEY SCHOOL

Contents

Overview

This E-Safety policy has been developed by the IT Committee made up of:

- Headteacher – Mr Richard Pollock
- E-Safety Officer/ Business Teacher / Data Compliance Manager – Mrs Jill Cosgrove
- Technical / IT Lead teacher – Mrs Anne-Marie Caporn
- DSL /Pupil Wellbeing Leader – Mrs Jill Pargeter
- Deputy Headteachers – Mrs C Lancaster and Mr Rob Morris
- Operations Manager – Mrs Clare Holt

Consultation with the whole school community has taken place and will continue to do so through a range of formal and informal meetings, typically through the following:

- Staff Meetings / INSET Days
- School Pupil Council
- IT Forum
- Anti-Bullying Steering Group
- Governors Meetings / Sub-committee Meetings
- School Website / Newsletters
- Cransley Google 'sites' - Intranet Pupil Hub & Teacher Hub
- Pupil Computer Science group

Scope of the Policy

This policy applies to all members of the Cransley School community (including staff, pupils, volunteers, parents/carers, visitors,) who have access to and are users of school ICT systems, both in school and out of school where actions relate directly to school set activity or use of school online systems.

The Education Act 2011 empowers the Headteacher, to such extent as is reasonable, to regulate the behaviour of pupils 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 out of school, but is linked to membership of the school. 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. This includes the four areas of risk found in KCSIE 2022:

- Content
- Contact
- Conduct
- Commerce

This Policy should be read in line with the following School policies amongst other important documentation. These can be found on the School website or on request from the School Office. https://cransleyschool.com/documents-and-policies

- Expectation For Learning / Behaviour Policy
- Acceptable User Agreements (Pupils and Staff)
- Safeguarding Child Protection Policy
- Anti-Bullying Policy
- RSE policy
- GDPR Policy
- Complaints Policy
- Employee Handbook

Roles and Responsibilities:

The following section outlines the roles and responsibilities for E-Safety of individuals and groups within the school:

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The Governors' Academic Committee will undertake the review.

The Governors in particular are aware that we have an appropriate firewall controlled by NSOptimum (Cransley School IT Support Services) and Web content filtering is controlled by Netsweeper software.

This is regularly monitored by the E-Safety Officer, DSL and the IT Lead teacher by testing the system and recording the findings in the Netsweeper on a termly basis. A log is available for analysis as required.

Headteacher and SMT

The Headteacher 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 E-Safety Officer.

The Headteacher will ensure that the E-Safety Officer and subsequently all relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.

The Headteacher and members of the SMT will receive a termly report from the E Safety Officer prior to the General Academic Committee or Full Board meetings.

The Headteacher and members of the Committee are aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff or pupil. (Reference Safeguarding Child Protection Policy)

E-Safety Officer

Cransley School has a named member of staff – Jill Cosgrove (JC) with a day-to-day responsibility for E-Safety. JC will work closely with SMT. She will:

- Ensure responsibility is shared amongst the members;
- Take day-to-day responsibility for E-Safety issues and take a leading role in establishing and reviewing the school E-Safety policies / documents;
- Receive reports of E Safety incidents and supports pastoral logs of incidents to inform future E Safety developments;
- Report termly to the Senior Management Team;
- Liaise with Cransley School IT Support Services/NSO.

ICT Technical Support

Cransley School has a managed ICT service provided by an external contractor, NSOptimum. It is the responsibility of the school to ensure that the managed service provider undertakes the following responsibilities:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- That the school meets required E-Safety technical requirements, both for in School and online learning (Google Classroom);
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed;
- The Firewall and Online filter protection systems (Netsweeper) are applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- That they keep up to date with E-Safety technical information to effectively carry out their E-Safety role and to inform and update others as relevant;
- That the use of the network / Internet / Google Classroom Virtual Learning Environment / Remote Access / email is regularly monitored in order that any misuse, attempted misuse can be reported to the Headteacher, Senior Leader or E- Safety Coordinator for investigation, action and sanction;
- That monitoring software (Netsweeper) / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

These users are responsible for ensuring that:

- They have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices, through relevant training, including TES Develop / Google online modules in e-safety, safeguarding, children protection and Child-on-Child abuse, including sexual harassment, sharing indecent images consensual and non-consensual and view and share pornography and other harmful content. They have an awareness of contact which could lead to pupils' being subjected to harmful online interaction with other users and an awareness of the dangers of commerce including online gambling inappropriate advertising and scams;
- They have read, understood and signed the Staff Acceptable Use Agreement (AUA) copies are kept in HR files

- They report any suspected misuse or problem to the Headteacher / Senior manager / E- Safety Officer/DSL for investigation / action / sanction and any necessary support of both perpetrators and victim;
- All digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- E-Safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the E-Safety and acceptable use agreements.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices;
- At all times, they take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse;
- They use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.

Designated Safeguarding / Pastoral Lead (DSL)

The DSL is trained in E-Safety issues and is aware of the potential for serious child protection issues which can arise from the use of the internet and ICT, and will address issues which arise in school or out of school. They will act in accordance with the procedures described in the Safeguarding Child Protection Policy, the Cheshire West and Chester SCP Procedures and KCSIE 2022, should any issue arise, particularly in relation to:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers / potential or actual incidents of grooming
- Cyber-bullying and prejudice-based bullying
- Sharing indecent images consensually or non-consensually
- Sexual harassment online
- The Prevent Duty
- viewing and sharing pornography and other harmful content

Acceptable User Agreements

Pupils:

Pupils are not permitted to have their mobile phones on their person during the school day. Phones are submitted to a central store on arrival. Failure to comply with this will result in disciplinary sanctions.

Pupils are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Agreements (AUA). The AUA's are sent out with the registration pack for all new pupils and collated by the Admission Officer. These can be found on the website
https://cransleyschool.com/documents-and-policies

Pupils must ensure:

- they submit their phones - locked and turned off - to the central store on arrival in school the phones are then locked under supervision in the main school office. Under exceptional circumstances pupils may need to gain high resolution photographs of their work and this would be carried out under close supervision of the subject teacher.
- they have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they develop resilience in how to protect themselves, and their peers, and understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- they report child-on-child abuse including sexual harassment, sharing indecent images both consensual and non- consensual and view and share pornography and other harmful content.
- they report any online bullying including prejudice based bullying;
- they are advised with regard to Cransley School policies on the use of Chromebooks, mobile phones, digital devices and handheld devices. They are also advised with regard to Cransley School policies on the taking / use of images and on cyber-bullying.

- 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-Safety Provision for Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in E-Safety is therefore an essential part of our school's E-Safety learning provision. Children and young people need the help and support of the school to recognise and avoid E-Safety risks and build their resilience. E-Safety education will be provided through a planned E-Safety programme as part of Computer Science / PSHEE/RSE, and is regularly revisited.

This is outlined in our scheme of work which covers each year group. This ensures that pupils are taught in all lessons to be critically aware of the materials they access on-line and be guided to validate the accuracy of information.

It also covers both the use of ICT and new technologies in school and outside school.

- Pupils resilience is built through a defined Computer Science and PSHEE/RSE curriculum and taught explicitly in Computer Science lessons, in PSHEE/RSE lessons, in assemblies, and in talks with visiting speakers (including the Cheshire Constabulary and CEOP, Safety Central and other providers, including the NSPCC)
- Pupils are helped to understand the need for the pupil AUA and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Rules for use of ICT systems / Internet are posted in all Computer Science rooms.
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

Assessment of how a pupil is progressing in matters of E-safety is taught within the Computer Science PSHE/RSE lessons is maintained through quality feedback and marking, with notes taken for progress and to address areas of concern individually or within small groups.

Where there is a pattern or groups of pupils who need intervention (across peer groups if necessary), specialist staff or external agencies will make provision and review learning opportunities.

Parents and Families

Parents and Carers, as Primary Educators, play a crucial part in keeping their children safe and are responsible for:

- Encouraging their child / children to follow the Pupil Acceptable Use Agreement at home, through the adherence to the Parental Acceptable User Agreement.
- Are encouraged to discuss E-Safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the Internet.
- Read updates from CEOP issued by the School.

E-Safety Provision for Parents and Families:

Parents and carers may have only a limited understanding of E-Safety risks and issues, yet they play 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 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).

The school therefore seeks to provide information and awareness to parents and carers through:

- Use of the Tooled up education Parent support library assisting with up-to-date research based approaches for home and school.
- Letters, newsletters, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Information is shared with parents as published by the E-Safety officer, IT Lead teacher and DSL in particular the following websites :

  The National Crime Agency's CEOP parent information think u know
  The National online safety campaign Wake up Wednesday

Technical – Infrastructure / Equipment, Filtering and Monitoring

The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It also ensures that the relevant people named in the Roles and Responsibilities sections are effective in carrying out their E-Safety responsibilities:

- School Servers are securely located and physical access is restricted.
- All users are provided with a username and password by the Network Manager who keeps an up to date record of users and their usernames. Users are required to change their password on a regular basis.
- School ICT technical staff may monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Agreements.
- Actual / potential E-Safety incidents are reported immediately to the E-Safety Officer who will arrange for these to be dealt with immediately in communication with the Technical Manager/DSL, reporting to the Headteacher.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations/ Chromebooks, and online protocols (Google Classroom) from accidental or malicious attempts which might threaten the security of the school systems and data. Web content filtering is by Netsweeper. Spam protection by Microsoft (org.uk addresses) and Google (.com email addresses).
- The school infrastructure and individual workstations are protected by up to date anti-virus software.
- Web content filtering is by Netsweeper. Spam protection by Microsoft (org.uk email addresses) and Google (.com email addresses).
- Advice is given to staff and pupils about ensuring they have password protection on all digital devices.

Google Classroom – Online Learning Environment

Please see the following documents for information about security and data protection whilst using G Suite for Education.
G Suite for Education FAQ - G Suite Admin Help

Curriculum

Where pupils are permitted to freely search the Internet, e.g. using search engines, staff are vigilant in monitoring the content of the websites the young people visit and encourage pupils to use specific appropriate search terms to reduce the likelihood of coming across unsuitable material.

Pupils are taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information and to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.

Use of Digital and Video Images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the Internet. However, staff and pupils / pupils need to be aware of the risks associated with sharing 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.

There are many reported incidents of employers carrying out Internet searches for information about potential and existing employees. The school informs and educates users about these risks and implements policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet eg on social networking sites
- Staff are permitted to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images
- Care should be taken when taking digital / video images that pupils / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website

Data Protection

Cransley School Ltd is a Data Controller as defined by the General Data Protection Regulation 2018 (GDPR) and as such has duties to use information or personal data it collects from individuals as part of its legitimate business activities in ways that protect the fundamental rights and freedoms of the individuals providing that information. GDPR applies to "*personal data*" which is defined as "*any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier such as a name, identification number, location data or similar*".

This information will be used to inform the normal business of running a school. In doing so we will:

- Only use personal data in ways that are lawful, fair and in a transparent manner,
- Only hold such data as is adequate, relevant and limited to what is necessary to carry out the legitimate activities of the school and safeguard pupils,
- Ensure that data is accurate and up to date. To this end we will issue confidential data collection check sheets annually.
- Keep data no longer than is necessary. Our Data Retention Guide is appended to the school's Data Protection Policy that can be found on the school website.
- Employ suitable and effective systems that ensure that personal data including sensitive information is kept secure against unauthorised access, loss, destruction or damage.

Staff must ensure that they:

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications:

A wide range of rapidly developing communications technologies have the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report to the nominated person – 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 pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Whole class or group email addresses will be used at KS1, while pupils / pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils 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 abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Responding to Incidents of Misuse:

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

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, and that members of the school community are aware that incidents have been dealt with.

If any pupil misuses the technological facility provided by the School (through online or in School) through a direct or indirect (but culpable) breach of the AUAs, sanctions will be put in place in line with the School Expectation for Learning and Behaviour Policy. For severe breaches or security and the AUA, these sanctions will include suspension of online or in-School technology access and use, alongside formal School based sanctions.

This can be found on the School website. https://cransleyschool.com/documents-and-policies

However, if any illegal misuse is detected or reported action will be taken in accordance with the guidance contained in the section entitled 'Procedures for dealing with Inappropriate/Illegal Internet Access or Material' in the Safeguarding Policy.

The Police and CEOP will be informed as soon as possible by the E-safety officer/DSL or any other member of staff in his absence with the Headteacher's knowledge and agreement, if any apparent or actual misuse appears to involve illegal activity, such as:

- Indecent images of children.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.
- Radicalisation
- sexual harassment
- sharing indecent images consensual and non-consensual
- view and share pornography and other harmful content.

Appendix 1: Social Media Policy

Introduction to Cransley School's Social Media Policy for Staff

Cransley School is aware and acknowledges that increasing numbers of adults and children are using social networking sites. The most commonly used social networking sites are Facebook, Instagram, Snapchat, WhatsApp and Twitter. Communicating content is also increasingly popular using YouTube, Vimeo and SoundCloud.

The widespread availability and use of social networking applications bring opportunities to understand, engage and communicate with audiences in new ways. It is important that we are able to use these technologies and services effectively and with a degree of flexibility, within the spirit of education rather than regulation. Cransley now has official pages on all these websites to harness the power to share and endorse content. However, it is also important to ensure that we balance such flexibility with our reputation.

In addition, recent changes to KCSIE (Keeping Children Safe in Education 2022) have placed an obligation on schools to ensure that the Staff Code of Conduct must cover staff/pupil relationships and communications including the use of social media.

Our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults. The policy requirements in this document aim to provide a balance to support innovation whilst providing a framework of good practice, which is echoed in our Staff Handbook. This policy takes account of employment legislation and best practice guidelines in relation to social networking in addition to the legal obligations of Governing Bodies and the relevant legislation.

Objectives

This policy sets out Cransley School's policy on social networking. New technologies are an integral part of our lives and are powerful tools, which open up teaching and learning opportunities for school staff in many ways.

This document aims to:

- Assist Cransley 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.
- Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use.
- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Support safer working practice.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.
- Reduce the incidence of positions of trust being abused or misused.
- Ensure that Cransley School is not exposed to legal risks.
- Ensure that the reputation of Cransley School is not adversely affected.

Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff will always advise the Headteacher of the justification for any such action already taken or proposed.

Scope

This document applies to all who work at Cransley School. This includes Teachers, Support Staff, Supply Staff, Administration Staff, Maintenance Staff, Governors, Volunteers and Contractors. It should be followed by any adult whose work brings them into contact with pupils. References to staff should be taken to apply to all the above groups of people in Schools. Reference to pupils means all pupils at Cransley School.
This policy should not be used to address issues where other policies and procedures exist to deal with them.

All Cransley School representatives should bear in mind that information they share through social networking applications, even if they are in private spaces, are still subject to copyright, Data Protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation.

Overview and Expectations

All adults working with pupils have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of pupils. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, pupils or students, public in general and all those with whom they work. Adults in contact with pupils should therefore understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting.

Staff are also reminded that they must comply with the requirements of equalities legislation in their on-line communications. Staff must never post inappropriate, derogatory or abusive remarks or offensive comments which may bring Cransley School – or any of its stakeholders - into disrepute.

Social media must not be used by staff to publish any content which may result in actions for defamation, discrimination, breaches of Copyright, Data Protection (GDPR) or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring Cransley School into disrepute.

Social media must not be used to discuss or advise any matters relating to School matters, staff, pupils or parents.

Any member of staff wishing to set up a social media presence in order to:

- aid School work or communication in an official manner,
- promote themselves professionally where the School's name is required, must inform the Headteacher prior to the creation of such an account to ensure continuity and to avoid duplication or any conflict of interest.

Safer Online Behaviour

Managing personal information effectively makes it far less likely that information will be misused.

- Staff should never publish personal information on social networking sites, such as addresses, home and mobile phone numbers. In addition, a Cransley email address should never be associated with a personal social media account.
- Staff personal profile settings should be set to maximise their privacy, to protect their professional reputation working in a School environment.
- Twitter users should ensure that their personal profile includes the line: "This is my personal account (and does not represent the views of Cransley School)". Staff should not follow pupils on Twitter
- Staff must take all reasonable steps to ensure that their personal information is secure; this means that no pupil should be able to freely search for or access their details. Staff should ensure that any inappropriate photographs are deleted from any profile.
- Staff should not be 'Friends' with, 'Followers' of, or connect with pupils on any social media network. It would be considered inappropriate to connect with pupils on a personal account. Depending on the circumstances, it may also be inappropriate to connect with parents, guardians or carers.
- Staff using Twitter in their official capacity can be followed by pupils but must ensure that content complies with the Staff Code of Conduct at all times and the School Policy on the use of images.
- Staff should never post anything that could be interpreted as glorifying or supporting terrorism, extremism or organisations promoting terrorist or extremist views, or encouraging others to do so.

Digital/Mobile Communication between Pupils / Cransley Staff

Communication between pupils and staff, by whatever method, should take place within clear and explicit professional boundaries outlined above and in the staff Code of Conduct (See Appendix 1 Safeguarding Policy). This includes the wider use of technology such as mobile phones, text messaging, emails, digital cameras, videos, web-cams, websites and blogs.

All communications between staff and pupils via social media will be performed using an account which is not the member of staff's personal account. If a member of staff is unsure how to set up a business/ professional account they should first gain permission and seek further guidance from the Assistant Head with responsibility for Systems and Data Management.