ALSTON MOOR FEDERATION

E-Safety Policy

Aim

To explain/set out the key principles expected of all members of the school community at Alston Moor Federation with respect to the use of ICT-based technologies.

Objectives

- Set out the key principles expected of all members of the school community at Alston Moor Federation with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of the Federation
- 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.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- 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.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

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

- **Content**

  - exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
  - lifestyle websites, for example pro-anorexia/self-harm/suicide sites
  - hate sites
  - content validation: how to check authenticity and accuracy of online content

- **Contact**

  - grooming
  - cyber-bullying in all forms
  - identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

- **Conduct**

  - privacy issues, including disclosure of personal information
  - digital footprint and online reputation
  - health and well-being (amount of time spent online (Internet or gaming))
  - sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
  - copyright (little care or consideration for intellectual property and ownership – such as music and film)
    (Ref Ofsted 2013)

This policy applies to all members of the Alston Moor Federation community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of Alston Moor Federation.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / 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 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 (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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 Responsibilities

Role	Key Responsibilities

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be aware of procedures to be followed in the event of a serious e-safety incident. • To receive regular monitoring reports from the E-Safety Co-ordinator / Officer • 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/IT support)
Deputy Headteacher/ E-Safety Co-ordinator / Designated Child Protection Lead	• To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents • promotes an awareness and commitment to e-safeguarding throughout the school community • ensures that e-safety education is embedded across the curriculum • liaises with school ICT support staff • To communicate regularly with the Headteacher and the designated e-safety Governor/Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident • To ensure that an e-safety incident log is kept up to date • facilitates training and advice for all staff • liaises with the Local Authority and relevant agencies • Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to 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 and use of social media
Governors / E-Safety/ Safeguarding governor	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety/Safeguarding Governor will include: regular review with the E-Safety Co-ordinator / Officer

Role	Key Responsibilities
	(including) e-safety incident logs, filtering / change control logs)
IT support	• To report any e-safety related issues that arises, to the Deputy Headteacher. • 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 • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis • that the use of the school network is regularly monitored in order that any misuse / attempted misuse can be reported to the Deputy Headteacher for investigation • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement • 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 • To report any suspected misuse or problem to the Deputy Headteacher • To maintain an awareness of current e-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Role	Key Responsibilities
Pupils	• Read, understand and adhere to the Pupil Acceptable Use Agreement • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • to understand the importance of reporting abuse, misuse or access to inappropriate materials • to know what action to take if they or someone they know feels worried or vulnerable when using online technology. • to know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • 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 • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home
Parents/ carers	• to support the school in promoting e-safety and endorse the Pupil Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images • to read, understand and promote the school Pupil Acceptable Use Agreement with their children • to access the school website in accordance with the relevant school Acceptable Use Agreement. • to consult with the school if they have any concerns about their children's use of technology

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year.

- Acceptable use agreements to be shared and signed by all staff, volunteers and governors at the start of each year and held in a central file

Handling Complaints

- 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.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - interview/counselling by tutor / Deputy Headteacher/ Headteacher;
  - informing parents or carers;
  - removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
  - referral to LA / Police.

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

- 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 child protection procedures.

Review and Monitoring

The e-safety policy is referenced from within other school policies: Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies.

- The school has an e-safety coordinator who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The e-safety policy has been written by the school e-safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

Education and Curriculum

- **Pupil e-safety curriculum**

  This Federation:

  - Has a clear, progressive e-safety education programme as part of the curriculum. It is build on LA e-safeguarding. This covers a range of skills and behaviours appropriate to their age and experience, including:

    - → To STOP and THINK before they click;
    - → to develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - → 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;
    - → to know how to narrow down or refine a search;
    - → to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - → 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;
    - → to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - → 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
    - → 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;
    - → to understand why they must not post pictures or videos of others without their permission;
    - → to know not to download any files – such as music files - without permission;
    - → to have strategies for dealing with receipt of inappropriate materials;
    - → to understand why and how some people will 'groom' young people for sexual reasons;
    - → 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.
    - → 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 CEOP button.

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an Acceptable Use Policy which every pupil will read and understand
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;

- Ensures that staff and pupils 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 / gambling.

Staff and Governor Training

This Federation:

- 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;
- Makes regular training available to staff on e-safety issues and the school's e-safety education program
- 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-safety policy and the school's Acceptable Use Agreements.

Parent Awareness and Training

This Federation:

- Runs a rolling programme of advice, guidance and training for parents, including:
  - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
  - Information leaflets
  - demonstrations, practical sessions held at school;
  - suggestions for safe Internet use at home;
  - provision of information about national support sites for parents.

Expected Conduct and Incident Management

- **Expected Conduct**

In this Federation, all users:

- 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.
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- 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
- 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** are responsible for reading the school's e-safety policy and using the school's ICT systems accordingly, including the use of mobile phones and handheld devices.

- **Pupils** should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- **Parents/Carers:**
  - should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at the time of their child's entry to the school;
  - Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Incident Management

In this Federation:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- 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.
- support is actively sought from other agencies as needed in dealing with e-safety issues
- 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, Governors /the LA
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

This Federation:

- Uses user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;

- Ensures network healthy through use of anti-virus software etc. and network set-up so staff and pupils cannot download executable files;
- Uses DfE/ LA approved systems, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Has appropriate blocks for sites which are deemed to be unsuitable/inappropriate for school
- Uses security time-outs on Internet access where practicable / useful;
- Works in partnership with the IT Support to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's system as a key way to direct students to age / subject appropriate web sites;
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the teacher.
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Network management (user access, backup)

In this Federation:

- Uses individual, audited log-ins for all users
- Requires the Technical Support to be up-to-date with LA services and policies;
- Storage of all data within the school will conform to the UK data protection requirements.

To ensure the network is used safely, this Federation:

- 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.
- We provide pupils with an individual network log-in username
- All pupils have their own unique username and password which gives them access to the Internet and school system
- Makes clear that no one should log on as another user and makes clear that pupils 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;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed.
- Has set-up the network so that users cannot download executable files / programmes;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- 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"
- Maintains equipment to ensure Health and Safety is followed
- Ensures that access to the school's network resources from remote locations by staff is restricted
- 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;
- Provides pupils and staff with access to content and resources through the approved school system which staff and pupils access using their username and password
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;

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

Password Policy

- This Federation makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

E-mail

This Federation:

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils or staff on the school website.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.

Pupils

- Pupils are introduced to and use e-mail as part of the ICT/Computing scheme of work.
- Pupils can only receive external mail from and send external mail to addresses if the rules have been set to allow this.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
    - 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;
    - that an e-mail is a form of publishing where the message should be clear, short and concise;
    - 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;
    - they must not reveal private details of themselves or others in email, such as address, telephone number, etc.;
    - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    - that they should think carefully before sending any attachments;
    - embedding adverts is not allowed;

- 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;
- not to respond to malicious or threatening messages;
- not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
- not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
- that forwarding 'chain' e-mail letters is not permitted.

- Pupils read and understand the school Agreement Form with the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff

- Staff only use the school e-mail system for professional purposes
- 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':
  - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
  - the sending of chain letters is not permitted;
  - embedding adverts is not allowed;
- All staff sign the school 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.

Federation Website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers;
- The school web site complies with the statutory DfE guidelines for publications;
- 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;
- 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;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

Social Networking

- 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, but to use the schools' preferred system for such communications.

- The Federation's preferred system for social networking will be maintained in adherence with the communications policy.

- Staff will ensure that in private use:
  - No reference should be made in social media to students / pupils, parents / carers or school staff
  - They do not engage in online discussion on personal matters relating to members of the school community
  - Personal opinions should not be attributed to the school or local authority
  - Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings, without permission except where disclosed to the Police as part of a criminal investigation.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

Data Security:

Management information System access and Data Transfer -

Strategic and operational practices

At this Federation:

- Staff are clear who are the key contact(s) for key school information (Headteacher/Deputy Headteacher) are.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record.

We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form.

- staff,
- governors,
- pupils
- parents

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

- We follow LA guidelines for the transfer of any data, such as MIS 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.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. / We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and school system access are working within the approved system and follow the security processes required by those systems.

Equipment and Digital Content -

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, student's & parents' 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.
- Student mobile phones which are brought into school must be turned off and stored out of sight during lessons. Staff and SKS Students may use their phones during school break times.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher/Deputy Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher/Deputy Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- 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.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone or out of lesson time. Staff may use their phones during break times.

- 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.
- 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.
- 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 member of staff.
- Personal mobile phones will only be used during lessons with permission from the teacher.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Students' use of personal devices

- 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.
- 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.
- 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.
- 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.
- 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.

Staff use of personal devices

- 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.
    - If members of staff have an educational reason to use mobile phones or a personally-owned device as part of an educational activity then all care should be taken to use school-based systems such as school email services.
- Staff should 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.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- 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 (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video

We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;

- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- 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 pupils;
- If specific pupil 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 pupil permission for its long term use
- Pupils 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 governors, parents or younger children as part of their ICT/Computing scheme of work;
- Pupils 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.
- Pupils 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 identify 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.

Monitoring Arrangements

This policy will be reviewed annually by the Governing Board.

Version Control	
Created by:	Headteacher
Approved by:	Full Governing Body
Date approved on:	November 2025
Next review due by:	November 2026