PRESTON PRIMARY SCHOOL

Online Safety Policy

Approved by Governors 15th December 2022

Review Date **July 2023**

Signed:

Headteacher: S. Richardson

Chair of Governors: C.Benjamin

Contents

1. Introduction and Overview

- Rationale and Scope
- Roles and responsibilities
- How the policy is communicated to staff/pupils/community
- Handling complaints
- Reviewing and Monitoring

2. Education and Curriculum

- Pupil online safety curriculum
- Staff and governor training
- Parent awareness and training

3. Expected Conduct and Incident Management

- Expected Conduct
- Staff, volunteers and contractors
- Parents/Carers
- Incident management

4. Managing the Information Technology (IT) Infrastructure

- Internet access, security (virus protection) and filtering
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Cloud environments (Google Drive)
- Social networking

5. Data Security

- Strategic and operational practices
- Technical Solutions

6. Equipment and Digital Content

- Mobile Devices (Mobile phones, tablets and other mobile devices)
- Storage, Synchronising and Access
- Staff use of personal devices
- Digital images and video

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Preston Primary School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and 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 for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be 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
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Online bullying in all forms
- Grooming (sexual exploitation, radicalisation etc.)
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of the Preston Primary School community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Preston Primary School IT systems, both in and out of Preston Primary School.

Roles and responsibilities

Role	Key Responsibilities
Headteacher/ Online Safety Co-ordinator/ Designated Child Protection Lead / Data and Information (Asset Owners) Managers (IAOs)	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant local and Trust guidance • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. Broadband provider • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident • Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • To receive monitoring reports from the Network Manager, where appropriate • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • To ensure school website includes relevant information. • KSCIE dictates that the DSL has overall responsibility for online safety – as a key part of the DSL remit
Headteacher/ Online Safety Co-ordinator/ Designated Child Protection Lead / Data and Information (Asset Owners) (IAOs) Managers	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the curriculum • Liaise with school technical staff where appropriate • To communicate regularly with SLT and the designated online safety Governor/committee to discuss current issues, review incident logs and filtering logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident

Role	Key Responsibilities
	• To ensure that online safety incidents are logged as a safeguarding incident • Facilitate training and advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues • Liaise with the Local Authority (LA) and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns. • To ensure that the data they manage is accurate and up-to-date, e.g. Management Information System (SIMS) • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • The school must be registered with Information Commissioner
Governors/Safeguarding governor (including online safety)	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the Online Safety Policy and review the effectiveness of the policy • To support the school in encouraging parents and the wider community to become engaged in online safety activities • The role of the online safety Governor will include: termly review meetings between the online safety Co-ordinator and Governor will take place.
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum • Liaise with school technical staff where appropriate
Network Manager/technician	• To report online safety related issues that come to their attention, to the Online Safety Coordinator • To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - 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 they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant

Role	Key Responsibilities
	• That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/ Headteacher • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures
Administration Staff	• To ensure that the Management Information System (SIMS) is accurate and up-to-date • That sensitive information is treated with respect and confidentiality – never leaving it open for others to view
Broadband provider nominated contact(s)	• To ensure all broadband provider services are managed on behalf of the school following data handling procedures as relevant • To ensure they uphold their contract to provide online monitoring/ filtering and provide the other services listed in their AUP
Teachers	• Adhere to all school policies • To embed online safety in the curriculum and school culture • 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 • Are responsible for ensuring children who do not have consent to appear in photos do not • Are responsible for ensuring children who do not have consent for photos to be shared on Seesaw are not posted • Are responsible for posting Seesaw safety and user message for parents • Are responsible for ensuring that children who do not have parental consent to access the internet do not do so • Ensure that all work-provided portable devices that contain photos or personal information/data about children are locked away when not in use. • Ensure that their log in credentials for all devices/services meet the requirements of the password policy and are not shared with anyone else

Role	Key Responsibilities
	• To ensure that any digital photos or personal information/data about children that are taken from the school premises are necessary for work purposes and encrypted (Either on school provided laptop, iPad or encrypted memory stick) • Ensure that all photos of pupils are taken on school devices (e.g. class camera or iPad) and that they are saved onto school provided encrypted server or storage, and deleted off the device promptly • Ensure only work related tasks are carried out on work provided devices • To ensure that they lock/log out of any work provided device when not actively using it. This applies to school online based services these include, but are not limited to, "CPOMS", "Gmail", "SIMS", "Evolve" • If staff access work online services on a personal device, staff have the responsibility to ensure that they have adequate password/pin protection
All school employed staff and volunteers	• Adhere to all school policies • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • Responsible for ensuring children who do not have consent to appear in photos do not • Ensure that all work-provided portable devices that contain photos or personal information/data about children are locked away when not in use. • Ensure that their log in credentials for all devices/services meet the requirements of the password policy and are not shared with anyone else • To ensure that any digital photos or personal information/data about children that are taken from the school premises are necessary for work purposes and encrypted (Either on school provided laptop, iPad or encrypted memory stick) • Ensure that all photos of pupils are taken on school devices (e.g. class camera or iPad) and that they are saved onto school provided encrypted server or storage, and deleted off the device promptly • Ensure only work related tasks are carried out on work provided devices • To ensure that they lock/log out of any work provided device when not actively using it. This applies to school online based

Role	Key Responsibilities
	services these include, but are not limited to, CPOMS, Gmail, SIMS, Evolve • If staff access work online services on a personal device, staff have the responsibility to ensure that they have adequate password/pin protection • To read, understand, sign and adhere to the school staff Acceptable Use Policy (AUP) , and understand any updates annually. The AUP is signed by new staff on induction. • To report any suspected misuse or problem to the online safety coordinator e.g. in person, using CPOMS • To maintain an awareness of current online safety issues and guidance e.g. through Continuous Professional Development (CPD) • To model safe, responsible and professional behaviours in their own use of technology **Exit strategy** • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Contractors/ Visitors	• Adhere to all relevant school policies • To read, understand, sign and adhere to the school visitors AUP
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy (Code of Conduct) annually • To understand how to use Seesaw appropriately for their class work and homework • 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 understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences

Role	Key Responsibilities
Parents/carers	• To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren • To consult with the school if they have any concerns about their children's use of technology • To support the school in promoting online safety and endorse the Visitors' Acceptable Use Policy and the Parental Online Safety 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 appropriate use of Seesaw to enhance their child's education
External groups including Parent groups	• Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school • To support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology. • To read, understand, sign and adhere to the school visitors AUP

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 included in the policy file in the school office.
- Policy folder on the school server system.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year
- Acceptable use agreements to be issued to whole school community, on entry to the school.
- Seesaw user agreement message to be posted for parents

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- DSL acts as first point of contact for any incident linked to safeguarding.
- Any suspected online risk or infringement is reported to Online Safety Coordinator that day
- Any concern about staff misuse is always referred directly to the Headteacher (DSL), unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Review and Monitoring

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Computing policy).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the Senior Leadership Team (SLT) and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing and PSCHE curriculum – in line with the RSE National Guidelines. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online 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 the pupil Acceptable Use Agreement (Pupil Code of Conduct);
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training

This school:

- makes regular training available to staff on online safety issues and the school's online 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 Online Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training

This school:

- Provides written guidance about how to keep their children safe when they are online.
- From time to time, the school will host parent sessions regarding online safety.
- The school will routinely post online safety updates through its social media channels and newsletters.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras;

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable
- know to take professional, reasonable precautions when working with pupils, previewing websites and apps before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the Parental Online Safety Agreement form;

Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the school 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;
- support is actively sought from other agencies as needed (i.e. the Local Authority, broadband provider, United Kingdom Safer Internet Centre helpline, (CEOP), Prevent Officer, Police, IWF), the ITSystems Team in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use is monitored;
- has the educational filtered secure broadband connectivity through the broadband provider;
- uses the broadband providers filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- ensures network health through use of anti-virus software;
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the broadband provider to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services e.g. supply teachers;
- Uses 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful;
- Has additional local network monitoring/auditing software installed;
- Ensures the Systems Administrator/network manager is up-to-date with relevant services and policies/requires the Technical Support Provider to be up-to-date with relevant services and policies;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to Department for Education DfE guidance;
- Storage of all data within the school will conform to the European Union (EU) and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's online 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 also provide a different username and password for access to our school's network.

- All pupils have their own unique username which gives them access to the Internet and other services, assuming parents have signed the relevant agreement;
- 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;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to log off/lock when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used only used to support their professional responsibilities.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;
  e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted;
- Our wireless network has been secured to appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy

- This school makes it clear that staff must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords as follows:
  - Is at least eight characters long.
  - Does not contain your user name, real name, or company name.
  - Does not contain a complete word.
  - Is significantly different from previous passwords.

    - Contains characters from each of the following four categories; Uppercase, lowercase, number, symbol
    - Further advice can be found at http://windows.microsoft.com/en-gb/windows-vista/tips-for-creating-a-strong-password
    - If staff feel they must write down their password in order to remember it, they are to make sure they don't label it as password, and are required to keep it in a safe place.

E-mail

This school

- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account;
- 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
- Uses a number of broadband provider-provided technologies to help protect users and systems in the school, including desktop anti-virus product

Pupils:

- We use a monitored and child level pupil email system which is delivered by our IT providers, ITSystems
- Pupils are taught about the online safety and etiquette of using e-mail both in school and at home.

Staff:

- Staff should only use school provided email systems on the school system
- Staff will use school provided e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained. This will be reviewed by the Trust annually.
- The school web site complies with statutory DFE requirements;
- 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;
- 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;

Shared Environments

- Uploading of information on the schools' sharded learning network space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;
- Access to networked areas when of site is through the use of the secure 'remote desktop' system.

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- 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.

School staff will ensure that in private use:

- No reference should be made in social media to present or former students/pupils, or parents/carers or school staff;
- School staff should not be online friends with any past or present pupil/student. Any exceptions must be approved by the Headteacher. This also extends to parents, unless the staff member was friends with this person prior to taking up post.
- 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 /academy or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our pupil Acceptable Use Agreement (Code of Conduct).

Parents:

- Parents are reminded about social networking risks and protocols through our parental Online Safety Agreement Form and additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people via written communication and verbal instruction

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO), with Chris Bracken, being our GDPR Officer.
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are Disclosing and Barring Service (DBS) checked and records are held in a single central record

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to lock/log-out of systems when leaving their computer
- All servers are in lockable locations and managed by DBS-checked staff. Keys for the server cabinet are securely stored when not in use.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- 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.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- 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 devices.
- No students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated and stored by the head teacher, handing back over to an adult with parental responsibility for the pupil
- Mobile devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- Personal mobile devices will not be used during lessons or pupil contact time unless as part of an approved and directed curriculum-based activity with consent from Headteacher / Senior Leadership Team. They should be switched off or silent at all times.
- The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices.
- No images or videos should be taken on personal mobile devices without the prior consent of the person or people concerned.
- Staff members may use their phones during pupil non-contact times, but only in appropriate areas where there are no children present, e.g. offices, staff room, PPA room.
- All visitors are requested to keep their phones on silent and not used in the presence of children.
- The recording, taking and sharing of images, video and audio on any **personal mobile** device is not allowed.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.
- 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.

Storage, Synching and Access

Work provided devices are only accessed with a school owned account

- Staff are to ensure only work related tasks and accesses to work related services are carried out on work provided devices
- Staff must sign a hardware loans agreement before taking devices off site
- If staff access work online services on a personal device, staff have the responsibility to ensure that they have adequate password/pin protection

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting, without express permission from the headteacher. If this is granted, staff must ensure their number is 'hidden' from the person receiving the call.

- Staff will be issued with a school phone where contact with students, parents or carers is required, for instance for off-site activities.
- 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.
- 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.
- 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 and then report the incident with the Headteacher / Designated Officer.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video

In this school:

- 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. Parents and withdraw this permission at any time. We will receive express permission to use these photographs for marketing / social media uses.
- 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;
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online 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 computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space – and are taught about age restrictions to sites and the reasons for these. 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 identity of others and

their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.