The Federation of St Bede's and St Bernadette Catholic Schools

WE LEARN, WE PLAY, WE CARE, WE PRAY

E-safety

Last review: March 2019

Next review: March 2021

FEDERATION VISION

Our vision is to provide all children with the best possible education, guided by the foundations of the Catholic faith, which develops their potential, prepares them for the future and inspires lifelong learning.

The Federation of St Bede's and St Bernadette Catholic Schools

St Bernadette Catholic Junior School

Adopted: March 2019 Review date: March 2021

Introduction

St Bernadette Catholic Junior School has a responsibility to keep pupils safe with our pupils being taught to: use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact (National Curriculum in England, Computing Programmes of Study, 2013; See appendix 1: Curriculum Coverage).

Main Aims

- To set out the key principles expected of all members of the school community at St Bernadette Catholic Junior School with respect to the use of ICT-based technologies.
- To safeguard and protect the children and staff of St Bernadette Catholic Junior School
- To 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.
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- To have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- To 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.
- To minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

These aims are set out in conjunction with the National Guidelines for E-Safety which is included within Appendix 3. Details regarding the use of email, mobile phone devices, tablets and data are all within this appendix.

How the subject is taught

St Bernadette Catholic Junior School has a clear, progressive e-safety education programme as part of the Computing curriculum. It is built on LA E-safeguarding and E-literacy framework for EYFS to Y6 national guidance, together with the Rising Stars Switched On Computing scheme of work. This covers a range of skills and behaviours appropriate to their age and experience (see Appendix 1: Curriculum Coverage; Pupil E-Safety Curriculum). E-Safety is taught alongside the Computing curriculum where teaching is supported by the E-Safety notes in the Switched on Computing Planning documents. An E-safety agreement is renewed annually for all staff and pupils, and is shared with parents (see Appendix 2: ICT Agreement).

Signed by:

________________________ **Subject Leader** **Date: ....**

Headteacher **Date: ....**

____

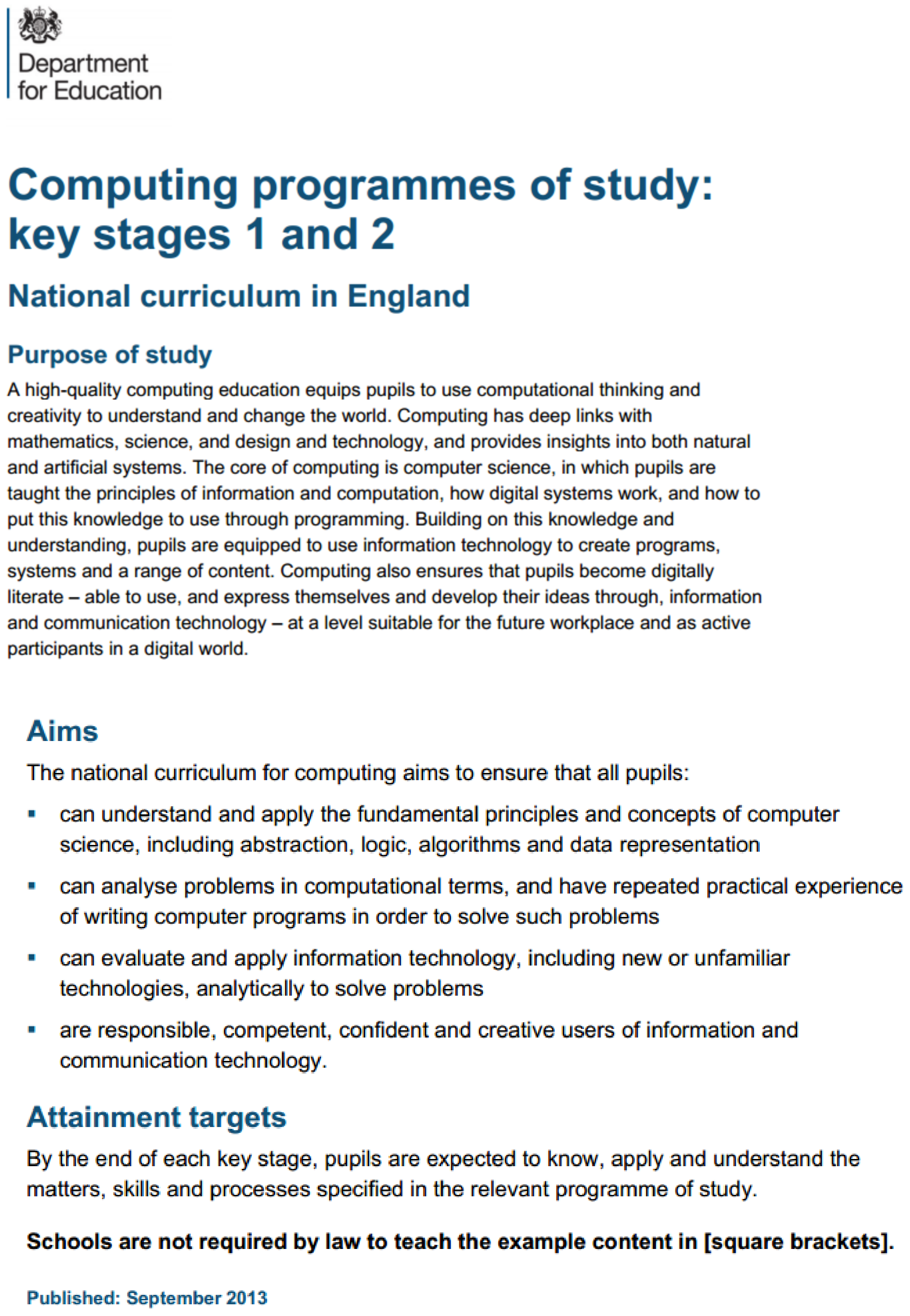
Chair of Governors **Date: ....**

____

This policy will be reviewed every two years.

Appendix 1: Curriculum Coverage

The E-Safety curriculum at St Bernadette Catholic Junior School directly follows the Computing Programme of Study for Key Stage Two as part of the National Curriculum in England.



Department for Education

Computing programmes of study: key stages 1 and 2

National curriculum in England

Purpose of study

A high-quality computing education equips pupils to use computational thinking and creativity to understand and change the world. Computing has deep links with mathematics, science, and design and technology, and provides insights into both natural and artificial systems. The core of computing is computer science, in which pupils are taught the principles of information and computation, how digital systems work, and how to put this knowledge to use through programming. Building on this knowledge and understanding, pupils are equipped to use information technology to create programs, systems and a range of content. Computing also ensures that pupils become digitally literate – able to use, and express themselves and develop their ideas through, information and communication technology – at a level suitable for the future workplace and as active participants in a digital world.

Aims

The national curriculum for computing aims to ensure that all pupils:

- can understand and apply the fundamental principles and concepts of computer science, including abstraction, logic, algorithms and data representation
- can analyse problems in computational terms, and have repeated practical experience of writing computer programs in order to solve such problems
- can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems
- are responsible, competent, confident and creative users of information and communication technology.

Attainment targets

By the end of each key stage, pupils are expected to know, apply and understand the matters, skills and processes specified in the relevant programme of study.

Schools are not required by law to teach the example content in [square brackets].

Published: September 2013

Key stage 2

Pupils should be taught to:

- design, write and debug programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts
- use sequence, selection, and repetition in programs; work with variables and various forms of input and output
- use logical reasoning to explain how some simple algorithms work and to detect and correct errors in algorithms and programs
- understand computer networks including the internet; how they can provide multiple services, such as the world wide web; and the opportunities they offer for communication and collaboration
- use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information
- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

Reference: DFE-00171-2013

Pupil e-safety curriculum

- 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.
- 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 school

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

Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
  - Introduction of the E-safety Policy and Agreement to new parents, to ensure that principles of e-safe behaviour are made clear
  - Information leaflets; in school newsletters; on the school web site;
  - suggestions for safe Internet use at home;
  - provision of information about national support sites for parents.

Appendix 2: ICT Agreement

PUPIL AND STAFF ICT AGREEMENT

SCHOOL COMPUTER, LAPTOP AND INTERNET USE

I understand that access to the Internet from St. Bernadette Catholic Junior School must be in support of educational research or learning, and I agree to the following:

- I understand I must only use the Internet and the computer for school work as directed by the teacher;
- I will ask permission from a member of staff before using the Internet;
- I will not record, video or photograph another person without their permission;
- I will only look at or delete my own files;
- I will not use internet chat in school.
- I will only e-mail people I know, or my teacher has approved;
- The messages I send will be polite and responsible;
- I understand that I must never give my home address or telephone number, or arrange to meet someone on the internet.
- If I see anything I am unhappy with, or I receive messages I do not like I will tell a teacher immediately;
- I will not delete this material but retain it as evidence;
- I understand that the school may check my computer files and may monitor the site I visit;
- I understand that there are safe and unsafe ways of using the Internet and I will keep myself safe;
- I will not use valuable Internet time playing non-educational games.
- I will not damage computers, computer systems or networks. Furthermore, if I discover any methods of causing such damage I will report them to a teacher.
- I will not attempt to change any computer, monitor or software settings on any school computers.
- If I violate any terms of this agreement, I will be denied access to the Internet and /or computers for a time to be determined by the Head teacher and may face further disciplinary action as determined by the Head teacher.

Name of the child: __________ Date: __________Class: ______________

Appendix 3: E-Safety Policy

Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant E-safety Policy and Agreement which they will be expected to sign before being given access to school systems. (at KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- 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 ICT systems accordingly, including the use of mobile phones, and hand held devices.

Pupils/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 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 school:

- 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, through the school's escalation processes.
- support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) 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 / LSCB
- 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 school:

- Has the educational filtered secure broadband connectivity through IES and so connects to the 'private' National Education Network;
- Uses the IES Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the pupils;
- Ensures network healthy through use of anti-virus software (from IES) etc. and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA or IES approved systems to send personal data over the Internet and uses encrypted devices or secure remote access where staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level;
- Works in partnership with the IES to ensure any concerns about the system are communicated so that systems remain robust and protect pupils;

- 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 pupils have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure
- Requires staff to preview websites before use [where not previously viewed or cached]; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search , …..
- 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 pupils that that they must report any failure of the filtering systems directly to the [*system administrator / teacher / person responsible for URL filtering]*. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or IES Helpdesk as necessary;
- 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)**
  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
  - Ensures the Systems Administrator / network manager is up-to-date with IES services and policies / requires the Technical Support Provider to be up-to-date with IES services and policies;
  - Storage of all data within the school will conform to the UK data protection requirements

    Pupils and Staff using mobile technology, where storage of data is online, will conform to the GDPR guidelines 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 e-safety Policy. Following this, they are set-up with Internet, email access and network access.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- We provide pupils with a class username.

- All pupils have access to a class username and their own school approved email account;
- 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;
- 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 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. We request that they DO switch the computers off at the end of the day.
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- 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" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by IES; equipment installed and checked by approved Suppliers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
  e.g. teachers access report writing module; SEN coordinator - SEN data;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child;
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- 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;
- Uses our broadband network for our CCTV system and have had set-up by approved partners;
- Uses the 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 or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);

- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- 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 school 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.
- Passwords for staff should be changed every 30 days e.g.

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;
- 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.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of IES-provided technologies to help protect users and systems in the school, including desktop anti-virus software, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. , Finally, and in support of these, IES filtering monitors and protects our Internet access.

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 SafeMail 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 e-mail, 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 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. They use Google supported Internet Legends guidelines to keep safe on line.

Staff:

- Staff only use the school e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- 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;

School 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 pupil use on a personal basis or to open up their own spaces to their pupils, 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 pupils / 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 pupil safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation.

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).

Through GDPR training staff are clear who are the key contact(s) for key school information 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 DBS checked and records are held in one central record

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

- 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 Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Equipment and Digital Content

Personal mobile phones and mobile devices

- 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.
- Staff members may use their phones during school break times.
  All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is not allowed. All mobile phone use is to be open to scrutiny and the Head teacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- 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 if there is good reason to believe such images are stored
- Where parents or pupils need to contact each other during the school day, they should do so only through the school office. Staff may use their phones during break times. 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 permission to use their phone at other than their 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 and put in a place of safety.

- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. hall or toilets.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones on school premises.
- No images, audio recordings or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Pupils' use of personal devices

- The School clearly states that pupil mobile phones should not be brought into school.
- If a pupil 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 only be released to parents or carers on request.
- If a pupil 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.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- No pupils should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.

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.
- Staff will be issued with a school phone where contact with pupils, parents or carers is required.
- 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 lessons.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos, audio recordings or videos of pupils 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.

NB. 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 pupils or parents, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

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 child 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 Agreement 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
- The school blocks/filter access to social networking sites or newsgroups;
- 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 scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any social media. 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.

Guidance for the use of Interactive White Boards (IWBs)

- Please do not attach personal devices (including mobile phones or tablets) to the interactive whiteboard at any time.
- If you use a school laptop or ipad to the IWB please ensure that they are logged off and removed at the end of use.

- The IWB may be used to show films and short clips in support of the curriculum.
- Only Universal (U) certificate films may be shown to pupils.
- Parental Guidance (PG) films or film clips may be shown with the consent of the Headteacher and parents in appropriate circumstances.
- All film content needs to have been checked by staff prior to viewing with pupils.

- **All films must be of good quality and pre approved by Senior Leaders**
- Films may be shown
  - during wet play sessions when two classes are together
  - during parent meetings as part of crèche provision
  - during parent evening (November and March)
  - Y3 for 'Movie Night' during the sleepover
  - Y6 at the end of SATs week
  - Y6 during school journey week
  - 1 film per Year Group at the end of each term (December, April and July)

- **Permission from the Headteacher must be sought to show any films other than the ones stated above.**