## 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 New Pastures Primary School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of New Pastures Primary School.
- 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.

This policy applies to all members of New Pastures Primary School community (including staff, students, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of the school ICT systems, both in and out of New Pastures Primary School. This policy has been based on the LGFL E-Safety Policy template 2015.

| Role | Key Responsibilities |
|---|---|
| Head teacher | • To take overall responsibility for e-safety provision<br>• To take overall responsibility for data and data security<br>• To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LA's filtered Internet Service<br>• To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant<br>• To be aware of procedures to be followed in the event of a serious e-safety incident.<br>• To receive regular monitoring reports from the E-Safety Co-ordinator<br>• 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) |

| Role | Key Responsibilities |
|---|---|
| E-Safety Co-ordinator / Designated Child Protection Lead | • takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents<br>• promotes an awareness and commitment to e-safeguarding throughout the school community<br>• ensures that e-safety education is embedded across the curriculum<br>• liaises with school ICT technical staff<br>• To communicate regularly with SLT and the designated e-safety Governor to discuss current issues and review incident logs<br>• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident<br>• To ensure that an e-safety incident log is kept up to date<br>• facilitates training and advice for all staff<br>• liaises with the Local Authority and relevant agencies<br>• Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:<br>  • sharing of personal data<br>  • access to illegal / inappropriate materials<br>  • inappropriate on-line contact with adults / strangers<br>  • potential or actual incidents of grooming<br>  • cyber-bullying and use of social media |
| Governors / E-safety governor | • To ensure that the school follows all current e-safety advice to keep the children and staff safe<br>• To approve the E-Safety Policy and review the effectiveness of the policy.<br>• To support the school in encouraging parents and the wider community to become engaged in e-safety activities<br>• The role of the E-Safety Governor will include:<br>  • regular review with the E-Safety Co-ordinator |
| Computing Curriculum Leader | • To oversee the delivery of the e-safety element of the Computing curriculum |
| Technician | • To report any e-safety related issues that arises, to the e-safety coordinator.<br>• 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<br>• To ensure that provision exists for misuse detection and malicious attack (e.g. keeping virus protection up to date)<br>• To ensure the security of the school ICT system<br>• To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices<br>• The school's policy on web filtering is applied and updated on a regular basis<br>• That he keeps up to date with the school's e-safety policy and technical information in order to effectively carry out his e-safety role and to inform and update others as relevant |

| Role | Key Responsibilities |
|---|---|
| | • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.<br>• To keep up-to-date documentation of the school's e-security and technical procedures |
| Office Manager | • To ensure that all data held on pupils on the school office machines have appropriate access controls in place |
| Teachers | • To embed e-safety issues in all aspects of the curriculum and other school activities<br>• To supervise and guide pupils carefully when engaged in learning activities involving online technology ( including, extra-curricular and extended school activities if relevant)<br>• 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<br>• To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy<br>• 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<br>• To report any suspected misuse or problem to the e-safety coordinator<br>• To maintain an awareness of current e-safety issues and guidance e.g. through CPD<br>• To model safe, responsible and professional behaviours in their own use of technology<br>• 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. |
| Pupils | • To know what action to take if they or someone they know feels worried or vulnerable when using online technology<br>• To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home |

| Role | Key Responsibilities |
|---|---|
| Parents/carers | • To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images<br>• To access the school website in accordance with the relevant school Acceptable Use Agreement.<br>• To consult with the school if they have any concerns about their children's use of technology |
| External groups | • Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school |

**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 to be issued to all staff/governors/volunteers/students to read and sign agreement at the beginning of the new school year or on entry to school

**Handling complaints:**

- The school will take all reasonable precautions to ensure e-safety.
- Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher, Mrs P Belnavis
- 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 / LA child protection procedures.

**Review and Monitoring**

The E-safety policy is referenced from within other school policies: ICT and Computing policy, Child Protection policy and Anti-Bullying policy.

- 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.

## 2. Education and Curriculum

### Pupil e-safety curriculum

The school

- Has a clear, e-safety education programme as part of the ICT and Computing curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - to STOP and THINK before they CLICK
    - to know how to narrow down or refine a search;
    - to understand acceptable behaviour when using an online environment, 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;
    - 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 understand 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 Child Line 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.

*Guidelines for safe use of the Internet are displayed in every classroom.*

### Staff and governor training

The 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 program through CPD and staff meetings

- 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**

The school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - 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.

## 3. Expected Conduct and Incident management

**Expected conduct**

At New Pastures Primary School:

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.
- 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 system
- 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

Pupils

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

Parents/Carers

- 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
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

**Incident Management**

At New Pastures Primary 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 by school
- support is actively sought from other agencies as needed (e.g. the local authority, 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.

- ○ 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.

## 4. Managing the ICT infrastructure

**Internet access, security (virus protection) and filtering.**

The school:

- ○ Has the educational filtered secure broadband connectivity provided by Doncaster Local Authority;
- ○ Works in partnership with the LA 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;
- ○ Ensures all staff have signed an acceptable use agreement form and understands that they must report any concerns;
- ○ Ensures pupils only publish within an appropriately secure environ
- ○ 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 , .....
- ○ Never allows / Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- ○ Informs all users that Internet use is monitored;
- ○ Informs staff that that they must report any failure of the filtering systems directly to the Head Teacher or E Safety coordinator;
- ○ 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)**

  The school:

  - ○ Ensures all storage of all data within the school will conform to the UK data protection requirements

*To ensure the network is used safely, the school:*

- Ensures staff 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;

- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- 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;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- 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;
- *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;
  e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / LA electrical engineers;
- 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
- 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 the DfES secure s2s website for all CTF files sent to other schools;
- 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.

  *See additional LA guidelines re transfer of data*

**Password policy**

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

## E-mail

**The school:**

- Provides staff with an email account for their professional use, *LA email* 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;
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.

**Staff**

- 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;

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

## School website

- The Head teacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- 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, admin@pittstreetinfant.doncaster.sch.uk;
- 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;

## Social media

School staff will ensure that in private use:

- No reference should be made in social media to 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.

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

### Strategic and operational practices

At this school:

- The Head Teacher, Mrs P Belnavis is the Designated Safety Officer and responsible for dealing with 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,
  - parent volunteers,
  - Students.

  This makes clear staff responsibilities with regard to data security, passwords and access.
- We follow LA guidelines for the transfer of any data, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- School staff with access to setting-up usernames and passwords for email and network 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.
- Staff have a secure area on the network to store sensitive documents or photographs.

*See Data Protection Policy*

## 6. Equipment and Digital Content

### Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, students & 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.
- Staff members may use their phones during school break times.
  All visitors are requested to keep their phones on silent.
- 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.
- 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.

***Staff use of personal devices***

- Staff handheld devices, including cameras must be noted in school – name, make & model, serial number.
- 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 students, 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 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.
- 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**
**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 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
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- 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.

**Asset disposal**

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.
All redundant equipment will be disposed of through an authorised agency.

Appendices
Acceptable use policy
Acceptable use guidelines for parents
ThinkuKnow Sid's top tips for using the Internet Safely
Becta AUP poster