William Hildyard Church of England Primary and Nursery School
E Safety Policy

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 William Hildyard with respect to the use of ICT-based technologies
- safeguard and protect the children and staff of William Hildyard
- 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 codes of practice relevant to responsible use of the Internet for educational, personal or recreational use
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- minimise the risk of misplaced or malicious allegations made against adults who work with students

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

<u>Content</u>

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

<u>Contact</u>

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

<u>Conduct</u>

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

(Ref Ofsted 2013)

Scope
This policy applies to all members of William Hildyard Primary and Nursery School community (including staff, students / pupils, volunteers, parents / carers and visitors) who have access to and are users of school ICT systems, both within and outside of school premises.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

Role	Key Responsibilities
Headteacher	• to take overall responsibility for e-safety provision • to take overall responsibility for data and data security • to ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements. • to be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • to be aware of procedures to be followed in the event of a serious e-safety incident. • to receive regular monitoring reports from the E-Safety Co-ordinator • to ensure that there is communication in place with the Network Provider to monitor and support staff who carry out internal e-safety procedures
E-Safety Co-ordinator	• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents • promotes an awareness and commitment to e-safeguarding throughout the school community (including parents) • ensures that e-safety education is embedded across the curriculum • liaises with the Network Provider • communicates regularly with SLT and the designated e-safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs • ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident • ensures that an e-safety incident log is kept up to date • facilitates training and advice for all staff • is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: ◦ sharing of personal data ◦ access to illegal / inappropriate materials ◦ inappropriate on-line contact with adults / strangers ◦ potential or actual incidents of grooming ◦ cyber-bullying and use of social media
Governors / E-safety governor	• to ensure that the school follows all current e-safety advice to keep the children and staff safe • to approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor • to support the school in encouraging parents and the wider community to become engaged in e-safety activities • the role of the E-Safety Governor will include: ◦ regular review with the E-Safety Co-ordinator / Officer (including e-safety incident logs, filtering / change control logs)

Role	Key Responsibilities
Computing Curriculum Leader	• to oversee the delivery of the e-safety element of the Computing curriculum • to liaise with the e-safety coordinator regularly
Network Provider	• to report any e-safety related issues that arises, to the e-safety coordinator. • to ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • to ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • to ensure the security of the school ICT system • to ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis • the Network Provider is informed of issues relating to the filtering • keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • that the use of the school network and email system is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Co-ordinator for investigation • to ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • to keep up-to-date documentation of the school's e-security and technical procedures • 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 • to supervise and guide pupils appropriately 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 • to report any issues in accordance with the Safeguarding Policy
All staff	• to read, understand and help promote the school's e-safety policies and guidance • to read, understand, sign and adhere to the school staff Acceptable Use Agreement • to report any suspected misuse or problem to the e-safety coordinator • to maintain an awareness of current e-safety issues and guidance e.g. through CPD • to model safe, responsible and professional behaviours in their own use of technology • to ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc. • to report any issues in accordance with the Safeguarding Policy

Role	Key Responsibilities
Pupils	• to read, understand, sign and adhere to the Pupil Acceptable Use Agreement. In Foundation Stage, staff will discuss and promote the KS1 Acceptable Use Agreement with pupils • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • to understand the importance of reporting abuse, misuse or access to inappropriate materials • to know what action to take if they or someone they know feels worried or vulnerable when using online technology • to know and understand school policy on the use of mobile phones, digital cameras and hand held devices • to know and understand school policy on the taking / use of images and on cyber-bullying. • to understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school • to take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • to help the school in the creation/ review of e-safety policies
Parents/carers	• to read, understand and promote the school Pupil Acceptable Use Agreement with their children • to consult with the school if they have any concerns about their children's use of technology
External groups, eg: Forest Schools	• any external individual / organisation will sign a Staff Acceptable Use Agreement 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
- Pupil Acceptable Use Agreements discussed with pupils at the start of each year.
- Staff Acceptable Use Agreements to be issued to whole school community, usually on entry to the school

Handling Complaints

- The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
    - Interview with E-Safety Coordinator;
    - informing parents or carers;
    - removal of Internet or computer access for a period;
    - referral to LA or Police.

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

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school child protection procedures.

Review and Monitoring
The e-safety policy will be reviewed every three years 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 SLT and approved by Governors and other stakeholders such as the PTA. All amendments to the school Safeguarding Policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Pupil E-Safety Curriculum

This school

- has a clear, progressive e-safety education programme as part of the Computing curriculum. It is built on LA guidelines and LGfL e-safeguarding. This covers a range of skills and behaviours appropriate to their age and experience, which is detailed in the Computing Policy
- plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- will remind students about their responsibilities through a Pupil Acceptable Use Policy which every student will sign and which will be displayed throughout the school and when a student logs on to the school network
- 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 or 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
- 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 Agreements.

Parent Awareness and Training

This school

- offers a range of advice and guidance for parents, including:
    - introduction of the Acceptable Use Agreements for children, to ensure that principles of E-safe behaviour are made clear
    - information in leaflets, school newsletters and on the school web site
    - suggestions for safe Internet use at home
    - offering E Safety workshops

3. 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 Acceptable Use Policy which they will sign before being given access to school systems (KS1 AUA for Foundation children)
- 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
- 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
- are expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices, in accordance with the Staff Acceptable Use Agreement
- staff have signed the iPad Agreement which is then held in their file

Incident Management

- in the event of an incident, the E Safety Co-ordinator will be informed
- the E Safety Co-ordinator will complete an Incident Form, located on the G drive
- if an incident breaches one of the Acceptable Use Agreements, appropriate sanctions will be issued in line with the Behaviour Policy
- all members of the school 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
- in the event of a significant incident, parents / carers of the children involved will be informed
- the Police will be contancted if one of our staff or pupils receives online communication that we consider raises any safeguarding concerns

4. Managing the ICT Infrastructure

Internet access, security (virus protection) and filtering

This school:

- has the educational filtered secure broadband connectivity through Lincolnshire CC.
- uses the LCC provided 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
- ensures network health through use anti-virus software (maintained by The Network Provider) and network set-up so staff and pupils cannot download executable files
- uses LA approved systems to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site
- blocks all Chat rooms and social networking sites
- only unblocks other external social networking sites (such as YouTube) for teachers only by request for specific purposes such as 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, such as Audio Network
- works in partnership with The Network Provider 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
- ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns
- ensures pupils only publish within an appropriately secure environment, such as the school's website or blog
- requires staff to preview websites before use

  is vigilant when conducting 'raw' image search with pupils e.g. Google image search
- informs all users that Internet use is monitored
- informs staff and students that that they must report any failure of the filtering systems directly to the e safety co-ordinator, who will escalate the issue as appropriate
- 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
- immediately refers any material we suspect is illegal to the appropriate authorities.

Network Management (user access, backup)

This school

- uses individual, audited log-ins for all staff users
- uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- ensures that the Network Provider is up-to-date with the school policies
- storage of all data within the school will conform to the UK data protection requirements. Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.
- 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
- 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 and we also switch off all computers at the end of the day to save energy
- 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 Network Provider 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, equipment installed and checked by the Network Provider or approved electrical engineers
- ensures that the school network is not accessible outside of school; work carried out by teachers off site will automatically synchronise when they enter school and switch on their computer
- 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, for example where training is being carried out
- daily back up of MIS system and other important files is carried out by the Network Provider; an email is sent to the e safety co-ordinator alerting her to any issues. This is fed back to the Network Provider to rectify.
- has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data
- 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
- 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 suitable for educational use
- all computer equipment is installed professionally and meets health and safety standards
- reviews the school ICT systems regularly with regard to health and safety and security.

Passwords

- this school makes it clear that staff must always keep children’s passwords private (for IT systems in use in school such as Purple Mash or Education City) and must not leave them where others can find them.
- all staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

E-Mail

This 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. We use anonymous or group e-mail addresses, for example enquiries@aspire.school for communication with the wider public

- will contact the Police if one of our staff or pupils receives an e-mail that we consider raises any safeguarding concerns
- will ensure that email accounts are maintained and up to date
- knows that spam, phishing and virus attachments can make e mails dangerous. The Network Provider provides technologies to help protect users and systems in the school, including desktop anti-virus, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language.
- 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

- 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. enquiries@aspire.school. 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

5. Equipment and Digital Content

Students' use of personal devices

- the School strongly advises that student mobile phones should not be brought into school.
- the School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- if a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- if a student needs to contact his or her parents or carers, they will be contacted by reception staff. Parents may not to contact their child via their mobile phone during the school day, but can pass a message on via the school office.
- students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

- 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 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
- 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

Asset Disposal

Details of all school-owned hardware will be recorded in a hardware inventory. All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen. 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.