Holt Primary Online Safety Policy

Writing and reviewing the Online Safety policy

This policy is part of the school's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

- Ofsted inspectors will always make a written judgement under leadership and management about whether or not the arrangements for safeguarding children and learners are effective.
- The school will identify a member of staff who has an overview of Online Safety.
- Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior leadership and approved by governors.
- The Online Safety Policy and its implementation will be reviewed regularly.
- The Online Safety Policy was discussed by staff during June 2016.
- The Online Safety Policy was revised by: Tom Gleeson.
- It was approved by the Governors on: 13th July 2016.
- Date of next review: June 2018.

Contents

Guidance and Supporting documents (separate documents):

Legal Framework

Pupil ICT Code of conduct

Staff, Governor and Visitor ICT Code of conduct

Parental/Carer Permission: Use of digital images

Parent/Carer ICT Code of Conduct agreement form

Guidance for schools: Parents & Carers use of photography at school events

Google Self-Certification Checklist Document

DfE Cloud Services Software and the Data Protection Act

Incident logging form

Online safety incident flowchart

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 Holt Primary with respect to the use of technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of technologies 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

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

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of Holt Primary community (including staff, students/pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of school technologies, both in and out of 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, including information and guidance where appropriate
- All staff must read and sign the 'Staff Code of Conduct' before using any school technology resource
- Regular updates and training on online safety for all staff, including any revisions to the policy
- ICT Code of Conduct discussed with staff and pupils at the start of each year. ICT Code of Conduct to be issued to whole school community, on entry to the school.

Handling Concerns

- The school will take all reasonable precautions to ensure online safety is in line with current guidance from the Department for Education (DfE)
- Staff and pupils are given information about infringements in use and possible sanctions
- Designated Safeguarding Lead (DSL) acts as first point of contact for any safeguarding incident whether involving technologies or not
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the concern is referred to the Chair of Governors

Review and Monitoring

The Online Safety Policy is referenced within other school policies (e.g. Safeguarding and Child Protection Policy, Anti-Bullying Policy, PSHE).

- The Online Safety Policy will be reviewed regularly 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.

Online Safety Group

- During the first review cycle we will look to setup an online safety group to take responsibility for the review and monitoring of all aspects of online safety. This group would include staff, governors, pupils and parents.

2. Education and Curriculum

Pupil online safety curriculum

This school:

- ➔ has a clear, progressive Digital Literacy education programme as part of the Computing curriculum. This covers a range of online safety skills and behaviours appropriate to their age and experience.
- ➔ will remind students about their responsibilities through the pupil ICT 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.

Staff and Governor training

This school:

- ➔ makes regular up to date training available to staff on online safety issues and the school's online safety education program.
- ➔ provides, as part of the induction process, all staff (including those on university/college placement and work experience) with information and guidance on the Online Safety Policy and the school's ICT Code of Conduct.

Parent/Carer awareness and training

This school:

- ➔ provides information for parents/carers for online safety on the school website.
- ➔ provides induction for parents which includes online safety.
- ➔ parents/carers are issued with up to date guidance on a regular basis.

3. Incident management

In this school:

- ➔ there is strict monitoring and application of the Online Safety Policy, including the ICT Code of Conduct and a differentiated and appropriate range of sanctions.
- ➔ support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Police, Internet Watch Foundation) in dealing with online safety issues.
- ➔ monitoring and reporting of online safety incidents takes place with using secure online form and contributes to development of 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 – i.e. Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security and filtering

In this school:

- ➔ we follow guidelines issued by the Department for Education to ensure that we comply with all requirements for filtered broadband provision.
- ➔ we take our Internet Service Provision (ISP) from Norfolk County Council; currently this service is backed by BT but this will soon change to UpData.
- ➔ our internet access is proactively monitored for attempts to access illegal or unsuitable content by netsweeper and we can track any such events.
- ➔ internet access is restricted to pupils, staff and school visitors. The school WiFi network is secured and all websites visited are logged.
- ➔ all pupil devices can only be used with a user account and software and configuration changes can be made by ICT shared services.
- ➔ anti-virus and malware protection is installed on all machines and is updated automatically to react to new threats.
- ➔ our data backups are resilient and tested regularly.

E-mail

This school:

- ➔ provides staff with an email account for their professional use, e.g. nsix.org.uk and makes clear personal email should be through a separate account.
- ➔ uses anonymous email addresses, for example head@, office@.
- ➔ will contact the Police if one of our staff or pupils receives an email that we consider is particularly disturbing or breaks the law.
- ➔ will ensure that email accounts are maintained and up to date.

Pupil email:

- We use school provisioned pupil email accounts that can be audited.
- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff email:

- Staff will use LA or school provisioned e-mail systems for professional purposes.

- Access in school to external personal email accounts may be blocked.
- We will never use email to transfer staff or pupil personal data unless it is protected with secure encryption.
- '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 school web site complies with statutory DfE requirements.
- Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the authors' identity or status.
- Photographs of pupils 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.

Cloud Environments

- Apps for Education accounts provisioned by Norfolk County Council and Google provide the pupils with email accounts, document creation tools and storage.
- Google stores this data in the cloud and in a checklist document they outline how they comply with the law.
- Further information contained in the DfE guidance for Cloud Software Services and the Data Protection Act.

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 school's preferred system for such communications.
- The use of any school-approved social networking will adhere to ICT Code of Conduct.

Pupils:

- Are taught about social networks, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to follow our pupil ICT Code of Conduct.

Parents/Carers:

- Parents/carers are reminded about social networking risks and protocols through our parental ICT Code of Conduct and additional communications materials when required.

5. Data Protection and Security

Management Information System access and data transfer

- Our MIS is provided by Pupil Asset and conforms to all relevant UK data security requirements.
- Staff whose work involves children's data are aware of best practice with regards to keeping it secure.

6. Equipment and Digital Content

Bring Your Own Device Guidance (BYOD) for Staff and Pupils

- We follow guidance from The Education Network (NEN) around Bring Your Own Device.
- There is not currently wide scale use of BYOD in school if and when that changes we will use the NEN guidance to support and develop this policy.

Digital images and video

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form annually.
- 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.
- Staff sign the school's ICT Code of Conduct and this includes a clause on the use of personal mobile phones/personal equipment.
- 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, high profile use