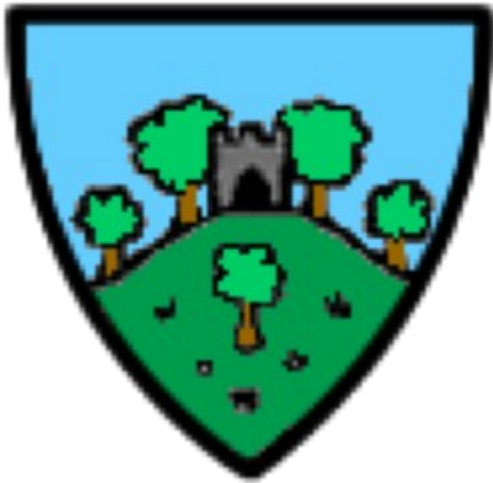




HOLTON LE CLAY SCHOOLS FEDERATION

Executive Head Teacher: Mrs D Hunt

Email: enquiries@holton-le-clay-infant.lincs.sch.uk

Email: enquiries@holton-le-clay-junior.lincs.sch.uk

Website: www.holtonleclayschools.co.uk

Online Safety & Social Media Policy

Prepared by	E Safety Committee
Approved by	Full Governing Body
Adopted/reviewed Date	November 2024
Version Number	10
Next Review Date	November 2027



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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. Through the Headteacher governors will receive information about any e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor: the governor responsible is Ms K. Farbrace.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community
- The Headteacher is responsible for ensuring that all staff receive suitable CPD to enable them to carry out their e-safety roles.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role.
- The Headteacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff - liaises with the Local Authority, liaises with school Computing technical staff, receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

Network Manager / Technical staff:

The school has an externally managed system and it is their responsibility as part of that contract to ensure

- That the school's Computing infrastructure is secure and is not open to misuse or malicious attack
- That the school meets the e-safety technical requirements as outlined in national guidance
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- That the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher

- That monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy / Agreement
- They report any suspected misuse or problem to the Headteacher / Senior Leader for investigation / action / sanction
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Students / pupils understand and follow the school e-safety and acceptable use policy
- They monitor Computing activity in lessons, extra curricular and extended school activities
- They are 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
- In lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- PSHE and computing complement each other in the teaching and monitoring of online safety and that PSHE allows discussion of online safety as well as in computing lessons. Relationship and friendship teaching will help positively reference online safety to ensure the link is made between positive behaviours at all times, especially when online.

A Designated person for child protection / Child Protection Officer - if not the Headteacher - should be trained in e-safety issues 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
- The 'Prevent' strategy.

It is important that all members of staff are aware of safeguarding issues arising from online safety.

Students / pupils:

- Are responsible for using the school Computing systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. There is another version of the Pupils Acceptable user policy for Key Stage 1
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- 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 understand the importance of adopting good e-safety practice when using digital technologies out of school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of Computing than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for endorsing (by signing) the Student / Pupil Acceptable Use Policy.

Visitors/volunteers

Anyone who visits the schools and who access school Computing systems will be made aware of and expected to sign the **Acceptable Users Agreement**.

Education - pupils

Whilst regulation and technical solutions are very important, we view the education of our pupils in e-safety as an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-Safety education will be provided in the following ways:

- An ongoing e-safety programme that is part of Computing / other lessons and will be regularly revisited – this will cover both the use of Computing and new technologies in school and outside school
- Pupils will be taught in lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils will understand the need for the pupil AUP and be encouraged to adopt safe and responsible use of Computing, the internet and mobile devices both within and outside school
- Rules for use of Computing systems / internet will be displayed around each school
- Staff will act as good role models in their use of Computing, the internet and mobile devices

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters and the web site
- Parents evenings
- Safeguarding and Remote Learning - Parents & Carers document
- Reference to any relevant websites.

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows.

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It

is expected that some staff will identify e-safety as a training need within the performance management process.

- All new staff should receive e-safety training ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings
- The Headteacher (or other nominated person) will provide advice / guidance / training as required to individuals as required

Training – Governors

Governors should take part in e-safety training / awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation.
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

It is the school's responsibility to ensure that the managed service provider carries out all the e-safety measures.

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- School Computing systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school Computing systems
Servers, wireless systems and cabling will be securely located and physical access restricted
- All users will have clearly defined access rights to school Computing systems. Details of the access rights available to groups of users will be recorded by the School Administrators.
- Pupils will always be supervised by members of staff when using IT.
- The “master / administrator” passwords for the school Computing system, used by the Network Manager (or other person) will be available to the Headteacher and School Administrator and kept in a secure place.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports a managed filtering service provided by Intalect/LA and is able to meet its statutory requirements to ensure the safety of staff / students / pupils) The school has provided enhanced user-level filtering through the use of the current filtering programme.
- In the event of the Network Manager needing to switch off the filtering for any reason, or for any user, this will be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).

- Any filtering issues should be reported immediately to LA
- Requests from staff for sites to be removed from the filtered list will be considered by the Subject Lead, Headteacher and School Administrator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly.
- The technical support contract includes regular monitoring and includes recording the activity of users on the school Computing systems and users are made aware of this in the Acceptable Use Policy.
- We have an appropriate system in place for users to report any actual / potential e-safety incident to the Headteacher
- There are appropriate security measures in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- A policy is in place discouraging the downloading of executable files by users since such files can easily carry a virus.
- A policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- A policy is in place that allows staff to install programmes on school workstations / portable devices.
- A policy is in place discouraging staff from the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices as staff cannot be sure what is contained on the media.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy Template in the appendix for further detail)

Curriculum

E-safety will be a focus in all areas of the curriculum and staff will reinforce e-safety messages in the use of Computing across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff will be vigilant in monitoring the content of the websites the young people visit and responding according to policy if the filtering system has allowed inappropriate material to be shown.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

- Students / pupils have access to the Pupil Share, where all Computing work will be saved. This is accessible by all members of staff and is to be regularly checked by the subject lead. This will be used to monitor the progress of Computing.

Curriculum - Infants

At the Infant school, we have access to range of online resources which are used to enhance the curriculum.

- Purple Mash is a resource that supports across the curriculum and is particularly useful in the teaching of coding.
- Charanga is an online portal used for teaching music. Its repetition is effective in recalling and learning. It offers a wide range of music and is supports teachers with an in-depth and well-structured scheme of work, which is able to be followed through the academic year.
- Yumu is the home learning resource of Charanga, a scheme used to teach Music. This mirrors the teaching of music within school.

Curriculum - Juniors

- Charanga is an online portal used for teaching music. Its repetition is effective in recalling and learning. It offers a wide range of music and is supports teachers with an in-depth and well-structured scheme of work, which is able to be followed through the academic year.
- Yumu is the home learning resource of Charanga, a scheme used to teach Music. This mirrors the teaching of music within school.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular we need to educate the children to recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes. If personal equipment is used to take photographs, they should be deleted as soon as possible.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the school policy (Use of Photographs Policy)
- Pupils' full names will not be used anywhere on a website or particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, X (formerly Twitter) and on Class Dojo.

- Pupil's work can only be published with the permission of the student / pupil and parents or carers. 6

Data Protection Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Details of procedures included in Data Protection Policies. This policy will soon be updated to reflect GDPR requirements.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Whole class or group email addresses may be used at KS1, while students / pupils at KS2 and above may be provided with individual school email addresses for educational use.
- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They will also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

Responding to incidents of misuse

It is expected that all members of the school community will be responsible users of Computing, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/ disciplinary procedures.

SOCIAL MEDIA

Holton le Clay Schools realise that social networking has become an integral part of everyday life and that many people enjoy membership of Social Network sites such as Facebook and X (formerly Twitter). However, we are also well aware that these sites can become a negative forum for complaining or gossiping and care must be taken not to breach our confidentiality policy or offend anyone when using these sites.

The following policy has been designed to give staff members clear guidance as to what we at Holton le Clay Schools expect of our staff when accessing these sites.

The absence of, or lack of explicit reference to a specific site does not limit the extent of the application of this policy. Where no policy or guidelines exists, employees should use their professional judgement and take the most prudent action possible. Consult with the Headteacher if you are unsure.

Breach of confidentiality will result in disciplinary action and may result in the termination of the employees contract.

There are four key areas:

- A. The use of social networking sites by pupils within school
- B. Use of social networking by staff in a personal capacity
- C. Comments posted by parents/carers
- D. Dealing with incidents of online bullying

A. The use of social networking sites by pupils within school

The school's Acceptable Use Policy (AUP) outlines the rules for using IT in school and these rules therefore apply to use of social networking sites. Such sites should not be accessed in school unless under the direction of a teacher and for a purpose clearly apparent from the learning objective of the relevant learning experience. If social media sites are used then staff should carry out a risk assessment to determine which tools are appropriate. Social Media sites to be used in school include blogging sites (Weebly Blog) and Twitter. Parents will give permission for children to access these sites in school as well as permission for images of their child / child's work to be included on the site. (See Social Media consent form).

In terms of private use of social networking sites by a child it is generally understood that children under the age of 13 are not permitted to be registered, including Facebook, Instagram and TikTok to name three.

B. Use of social networking by staff in a personal capacity

It is possible that a high proportion of staff will have their own social networking site accounts. It is important for them to protect their professional reputation by ensuring that they use their personal accounts in an appropriate manner.

When using social network sites staff/governors should give due regard to the following:

- Staff must never add pupils as 'friends' into their personal accounts- including past pupils under the age of 16.
- Staff are strongly advised not to add parents as 'friends' into their personal accounts.
- Staff must not post comments about the school, pupils, parents or colleagues- including members of the Governing Body.
- Staff must not use social networking sites within lesson times (for personal use).
- Staff should only use social networking in a way that does not conflict with the current National Teacher's Standards.
- Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality.
- Staff should read and comply with 'Guidance for Safer Working Practice for Adults who Work with Children and Young People'.
- Inappropriate use by staff should be referred to the Headteacher in the first instance and may lead to disciplinary action.
- Personal blogs should have clear disclaimers that the views expressed by the author of the blog is the author's alone and do not represent the views of Holton le Clay Schools.
- Information published on your blogs should comply with the Confidentiality Policy and disclosure of proprietary data policies. This also applies to comments posted on other blogs, forums and social networking sites.
- Always be respectful to Holton le Clay Schools, other staff members, parents and relatives, children. Staff should be aware that any disrespectful comments to the above may be considered libellous.
- Social media activities should not interfere with work commitments.
- Do not reference or cite Holton le Clay Schools, parents or children without their express consent.
- Remember at all times in or out of working hours you are an ambassador for Holton le Clay Schools and your online presence reflects on the setting.
- Any employee who becomes aware of social networking activity that would be deemed distasteful should make the Headteacher or Chairperson aware.

C. Comments posted by parents/carers

Parents and carers will be made aware of their responsibilities regarding their use of social networking. Methods of school communication include the prospectus, the website, newsletters, letters and verbal discussion. School policies and documents provide further information regarding appropriate channels of communication and means of

resolving differences of opinion. Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for the child.

Parents must not post pictures of pupils, other than their own children, on social networking sites where these photographs have been taken at a school event. Parents should make complaints through official school channels rather than posting them on social networking sites.

Parents should not post malicious or fictitious comments on social networking sites about any member of the school community.

D. Dealing with incidents of online bullying/inappropriate use of social networking sites

The school's Anti-Bullying Policy sets out the processes and sanctions regarding any type of bullying by a child on the school roll.

In the case of inappropriate use of social networking by parents, the Governing Body will contact the parent asking them to remove such comments and seek redress through the appropriate channels such as the Complaints Policy and will send a letter.

The Governing Body understands that, "There are circumstances in which police involvement is appropriate. These include where postings have a racist element or where violence is threatened or encouraged." Furthermore, "Laws of defamation and privacy still apply to the web and it is unlawful for statements to be written...which:

- Expose (an individual) to hatred, ridicule or contempt
- Cause (an individual) to be shunned or avoided
- Lower (an individual's) standing in the estimation of right-thinking members of society or
- Disparage (an individual in their) business, trade, office or profession." (National Association of Headteachers)

Policy breaches:

Staff found to be in breach of this policy may be subject to disciplinary action, in accordance with the School's Disciplinary Policy & Procedure and the Code of Conduct and Disciplinary Rules, with potential sanctions up to and including dismissal. Information shared through social networking sites, even on private spaces, is subject to copyright, data protection, freedom of information, equality, safeguarding and other legislation. Where staff work in roles that are governed by professional bodies/professional codes of conduct; the professional rules relating to social networking applied to them may be more stringent than those within this Policy.

HOLTON-LE-CLAY SCHOOLS FEDERATION STAFF, GOVERNOR AND VISITOR ACCEPTABLE USE AGREEMENT/CODE OF CONDUCT

Computing and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of Computing. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher / Governor ESafety co-ordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.

- I will comply with the Computing system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on MIS system Integris) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without permission of the Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carers, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- Staff must never add pupils as 'friends' into their personal accounts (including past pupils under the age of 16).
- Staff are strongly advised not to add parents as 'friends' into their personal accounts.
- I will support and promote the school's E-Safety and Social Media policy and help pupils to be safe and responsible in their use of Computing and related technologies.
- Use of mobile phones by staff in session time:
- As a general rule, staff should not have mobile phones on their person, or be using a phone, during session time. However, it is recognised that on rare occasions, the use of mobile phones might be appropriate. Examples might include a check on timings, use of alarms or to activate educational software