



Faldingworth Community Primary School
Normanby-by-Spital Primary School



Fair Acres
Federation
Our values and learning
are stronger together

Online Safety Policy

Adopted: 22nd January 2026

Review date: January 2027

Signed: (Chair of
Governors)

Signed:
(Headteacher)

New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter. The schools in the Fair Acres Federation endeavour to highlight benefits and risks of using technology and provides Safeguarding and education for users to enable them to control their online experience.

This policy operates in conjunction with the following school policies and procedures:

- Child Protection and Safeguarding Policy
- Whistleblowing policy
- Behaviour Policy
- Anti Bullying Policy
- Staff code of conduct
- Data Protection

The following local/national guidance should also be read in conjunction with this policy:

- PREVENT Strategy HM Government
- Keeping Children Safe in Education DfE September 2025
- Working together to Safeguard Children
- Learning together to be Safe: A Toolkit to help Schools contribute to the Prevention of Violent Extremism.

Safeguarding is a serious matter; at the schools in the Fair Acres Federation (Faldingworth and Normanby Primary Schools) we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as online safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an online safety incident, whichever is sooner.

The primary purpose of this policy is two-fold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any possibility of harm to the student or liability to the school.

This policy is available for anybody to read on the relevant school website (Faldingworth or Normanby); upon review all members of staff will sign as read and understood both the online safety policy and the Staff Acceptable Use Agreement. A copy of this policy and the Students Acceptable Use Agreement will be sent home with students at the beginning of Key Stage 1 and 2 with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in our schools but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

- We will provide a curriculum/other lessons which has online safety related lessons embedded throughout.
- We will celebrate and promote online safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant online safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.

- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objective for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an Acceptable Use Policy which every pupil will sign.
- School staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- Pupils will be taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying. See Anti-Bullying Policy.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

Remote/Home Learning

- We will endeavour to ensure that pupils continue to receive a good level of education 'beyond the classroom' by providing a range of resources via our website and learning portals.
- We expect pupils to follow the same principles, as outlined in the school's Acceptable User policy, whilst learning at home.
- If our school chooses to communicate with pupils via Google Meet, then it is important that this is only carried out with the approval of the Headteacher or Senior Leader. Pupils must uphold the same level of behavioural expectations, as they would in a normal classroom setting.
- Any significant behavioural issues occurring on any virtual platform must be recorded, reported and appropriate sanction imposed, which may include temporarily suspending access to group online learning. For all minor behavioural incidents, these should be addressed using the normal restorative approaches.
- Staff should be mindful that when dealing with any behavioural incidents, online, opportunities to discuss and repair harm will not be the same as if the child or young person was in school. Therefore, it may be necessary to have a discussion with the parents/carers, regardless how minor the incident, to ensure the child is emotionally well supported.

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any online safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of online safety at the school who will:
 - Keep up to date with emerging risks and threats through technology use.
 - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.
 - Receive monitoring reports on the implementation of the policy.
 - Help promote online safety in the wider community.
 - Challenge the school's policy and practice.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for online safety within our schools. The day-to-day management may be delegated to a member of staff, the online safety Officer, currently the computing subject lead.

The Headteacher will ensure that:

- Online safety training throughout the schools are planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated online safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All online safety incidents are dealt with promptly and appropriately and are logged and monitored.
- National online safety and National College provide material and opportunities for directed and self-directed CPD.

Online safety Officer

The online safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher and governing body on all online safety matters.
- Engage with parents/carers and the school community on online safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the online safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Monitor incidents and handle sensitive issues.
- Ensure any technical online safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make him/herself aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.
- Liaise with the headteacher about staff training.
- Ensure staff take responsibility for class online safety.

ICT Technical Support Staff – Education Lincs

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
 - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
 - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
 - Any online safety technical solutions such as Internet filtering are operating correctly.
 - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the online safety officer and Headteacher.
 - Support is given through regular visits to school where full requirements are discussed including any changes or problem solving with the onsite engineer and through remote support at any time as needed
 - Upgrades and installations are also discussed as are the existing policies and infrastructure

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood, it should be brought to the attention of the Headteacher.
- Any online safety incident is reported to the online safety Officer (and an online safety Incident report is made), or in his/her absence to the Headteacher. If you are unsure, the matter is to be raised with the online safety Officer or the Headteacher to make a decision.
- Online safety is taught throughout the year but also as/when online safety issues arise.

All Students

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

Online safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly, all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents/carers play the most important role in the development of their children; as such the school will ensure that parents/carers have the skills and knowledge they need to ensure the safety of children outside the school environment. Through working together meetings, school newsletters and Parent Mail / Parent Hub, the school will keep parents/carers up to date with new and emerging online safety risks and will involve parents/carers in strategies to ensure that students are empowered.

Parents/carers must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents/carers will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Personal use of social media by Parents and Carers

The school encourages all members of the community in the same responsible and respectful use of social media that is taught to pupils. All matters regarding the school are to be communicated via appropriate channels (see complaints procedure) so that they may be dealt with fairly and effectively for all concerned. Abusive, libelous or defamatory comments on social media regarding the school, staff or pupils will be reported to the site's 'report abuse' section for immediate removal.

Complaints Procedure

If a parent/carer or member of staff has any concerns or complaints with regard to social media, an appointment can be made by them to speak to a member of the school leadership team, who will investigate the complaint and if necessary will be able to advise on formal procedures for complaint.

Screening, Searching and Confiscation

The Education Act 2011, allows staff to lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

- cause harm,
- disrupt teaching,
- break school rules,
- commit an offence,
- cause personal injury, or
- damage property.

Technology

The schools in the Fair Acres Federation use a range of devices including PC's, Laptops, iPads and Chromebooks. Pupils are not permitted to bring personal devices to school. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use Cisco Meraki All in One Firewall and Filtering Solution with Advanced Malware Protection that prevents unauthorized access to illegal and inappropriate websites. The internet filtering software is monitored and regular updates and changes are applied to the system to ensure the internal network is securely protected and browser searching remains consistently monitored. Our IT helpdesk is available to log any changes to the filtering in regards to URL blocking and searching which devices are accessing what content.

Our filtering links together with the onsite server for policy management – there are 3 groups Admin, Staff and Standard Restricted Policies/Pupils. Devices to be used by pupils are set to the standard restrictions and are moved to the required policies only by request of staff. Any devices connected to the Guest Wifi are set to the standard restrictions and are moved to the required policies only by request of staff. Staff mobile devices are also recorded when accessing the Google Workspace Content.

If any inappropriate content is accessed or flagged by the school to the IT Helpdesk, Education Lincs will work actively with the school to find out what has happened. However, any attempts to access inappropriate content is usually blocked by the filtering before it can be accessed.

Senso - Senso Safeguard Cloud is designed to protect users utilising school-owned devices by proactively monitoring and alerting relevant staff to users who may be vulnerable or at risk, users who may pose a risk to others, as well as inappropriate or harmful behaviour.

Email Filtering – we Cisco Meraki All in One Firewall and Filtering Solution with Advanced Malware Protection to protect the school from infected emails being sent or received. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message. We also have Google's own in-built safeguards and antimalware/antispam protection. Any emails that contain potentially harmful content or are suspicious are blocked at entry and placed into a quarantine for review.

Protection - All school devices that hold personal data (as defined by the Data Protection Act 1998 and the recently updated General Data Protection Regulations of 2018) are password protected and encrypted. No data is to leave the school on a device that is not password protected or encrypted; all devices that are kept on school property and which may contain personal data are password protected and encrypted. Any breach (i.e. loss/theft of device such as laptop or USB key drives) is to be brought to the attention of the Headteacher immediately. Where possible staff should use the secure cloud storage solution that has been set up (Office 365 or Google Workspace) in place of using a memory stick. Any network access will require user identification for all users. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office in the event of a breach.

Passwords – all staff and students will be unable to access any device without a unique username and password. Passwords will be changed regularly or if there has been a compromise. The Headteacher and IT Support will be responsible for ensuring that passwords are changed. Staff are informed how to ensure passwords are high strength. Information will be locked after a number of unsuccessful attempts. Any incidents of password compromise will be reported and logged.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated and reviewed to ensure effectiveness. Our IT Support provider will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns.

Safe Use

Internet – Internet use is granted: to staff upon signing this online safety and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Photos and videos – Digital media such as photos and videos are taken on school equipment only that does not leave the school. All parents/carers must sign a photo/video release slip when the children start school; non-return of the permission slip will not be assumed as acceptance. Digital media will be used to promote quality of learning and children are educated about the risks involved. All digital media will be disposed of in accordance with the Data Protection Act.

Social Networking – there are many social networking services available; We are fully supportive of social networking as a tool to engage and collaborate with parents/carers and the wider school community. Computing curriculum will include a planned programme of education in relation to apps used by the children; the risks involved and content.

Blogging

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be “followed” or “friended” on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permission slips must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are “comment enabled”, comments are to be moderated.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner’s permission has been granted or there is a license which allows for such use.

Notice and take down policy – should it come to the school’s attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Digital Literacy – pupils are taught to practice skills of safe online behaviour. The planning of digital literacy complements the online safety program.

Incidents - Any online safety is to be brought to the immediate attention of the online safety Officer or the Headteacher. The Headteacher or the online safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log. Online safety incidents outside of school which effects the welfare of children or staff are also encouraged to be brought to the attention of the online safety officer via e-mail or in person. Because incidents are recorded this enables online safety to be audited and therefore revised in response. Incidents outside of school will be encouraged to be reported through email at school.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, we will have an annual program of training which is suitable to the audience in addition to online CPD and updates.

Online safety for students is embedded into the curriculum; whenever ICT is used in the school, staff

will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning. It is encouraged to promote online safety in PSHE and Computing lessons in all years. Online safety will be taught in response to incidents but also following a planned online safety program. The online safety curriculum will include; personal, social and technical issues that are current, relevant and new.

As well as the program of training we will establish further training or lessons as necessary in response to any incidents.

The Headteacher and online safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT 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 ICT. 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 Head Teacher and school online safety coordinator.

- 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 ICT 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 Integris) is kept secure and 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 carer, 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.
- I will support and promote the school's online safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.
- We do not permit the use of private emails.

✂.....

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature.....Date.....

Full Name..... (printed) Job title.....

Acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school's ICT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

I will not bring a personal mobile phone, smartwatch or other personal electronic device which has internet connectivity into school.

I will not bring any device on which photographs can be taken into school.

I agree that the school will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for bringing personal electronic devices into school, and will make sure my child understands these.

Signed (parent/carer):

Date:

Letter to Parents:

Dear Parent/Guardian

Use of the Internet in school is a vital part of the education of your child. Our school makes extensive use of the Internet in order to enhance their learning and provide facilities for research, collaboration and communication.

You will be aware that the Internet is host to a great many illegal and inappropriate websites, and as such we will ensure as far as possible that your child is unable to access sites such as this. We are able to do this using advanced software known as an Internet filter. This filter will categorise websites in accordance with their content; the school allows or denies these categories dependent upon the age of the child.

The software also allows us to monitor Internet use; the Internet filter keeps logs of which user has accessed what Internet sites, and when. Security and safeguarding of your child are of the utmost importance in our school; in order to ensure that there have been no attempts of inappropriate Internet activity we may occasionally monitor these logs. If we believe there has been questionable activity involving your child, we will inform you of the circumstances.

We explain the importance of Internet filtering to your child. Furthermore, we explain that there has to be a balance of privacy and safety; we also inform them that we can monitor their activity. All children are given the opportunity to ask questions and give their viewpoint. We would like to extend that opportunity to you also; if you have any questions or concerns please contact enquiries@normanby.lincs.sch.uk or enquiries@faldingworth.lincs.sch.uk.

We have included an Acceptable Use Agreement for parents/carers and pupils to sign – one for each pupil. Please can this be signed and returned to school by . The online safety policy is on our website.

Yours Sincerely

Mrs K Grummell

I have read this letter and understand that my child's Internet access will be monitored to ensure that there is no illegal or inappropriate activity by any user of the school network. I acknowledge that this has been explained to my child and that he/she has had the opportunity to voice their opinion, and to ask questions.

I have signed and returned the Acceptable Use Agreement by Please Tick

Name of Parent/Guardian –

Name of Child –

Signature -

Date