Acceptable User Policy

Status	Date
Date issued	May 2025
Prepared by	Janis Williams
Date reviewed	
Review date	May 2027
Date adopted by Governing Body	To be adopted May 2025

Inspire, Make a Difference, Persevere, Succeed

1. Introduction and Aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors;
- Establish clear expectations for the way all members of the school community engage with each other online;
- Support the school's policy on data protection, online safety and safeguarding;
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems;
- Support the school in teaching pupils safe and effective internet and ICT use.

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our disciplinary policy in the case of staff or behaviour policy for children.

2. Relevant Legislation and Guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2018
- Searching, screening and confiscation: advice for schools

3. Definitions

- **ICT facilities:** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service.

- **Users:** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose.
- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities.
- **Materials:** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs.

4. Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright;
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination;
- Breaching the school's policies or procedures;
- Any illegal conduct, or statements which are deemed to be advocating illegal activity;
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate;
- Activity which defames or disparages the school, or risks bringing the school into disrepute;
- Sharing confidential information about the school, its pupils, or other members of the school community;
- Connecting any device to the school's ICT network without approval from authorised personnel;
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data;
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel;
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities;
- Causing intentional damage to ICT facilities;
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel;
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation;
- Using inappropriate or offensive language;
- Promoting a private business, unless that business is directly related to the school;
- Using websites or mechanisms to bypass the school's filtering mechanisms;
- Using AI tools and generative chatbots (such as ChatGPT) to complete assessments, homework or to present AI-generated text or imagery as their own.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

This permission must be sought prior to engaging in any activity that is deemed unacceptable. Failure to do so may be dealt with under the disciplinary policy.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on Staff Behaviour Policy.

This may result in revoking permission to use the school systems.

This policy must be read in conjunction with: Staff Code of Conduct; Staff Disciplinary Policy; Social Media Policy.

5. Staff (including governors, volunteers and contractors).

5.1 Access to school ICT facilities and materials

One IT manages access to the school's ICT facilities and materials for school staff, with oversight from headteacher. That includes, but is not limited to:

- Computers, tablets and other devices;
- Access permissions for certain programmes or files.

Staff will be provided with unique log-in/account information and passwords (which can be reset) that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the headteacher or deputy head in their absence.

Should staff require access to files they are not currently authorised to see, this must be done through the headteacher.

5.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. See appendices for email protocol.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the headteacher or deputy head in their absence and immediately and follow school's data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The headteacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching or directed time;
- Does not constitute 'unacceptable use', as defined in section 4;
- Takes place when no pupils are present;
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes.

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's Mobile Phone Use Policy.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity. To be read in line with the Social Networking Policy.

5.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times. This policy must be read in conjunction with the Social Networking Policy.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely:

- This is managed by One It, with oversight of the headteacher;
- Staff remote access is via provided login details and dual authentication;

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the head teacher or One IT may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

This policy must be read in conjunction with the Data Protection Policy.

5.4 School social media accounts

The school has an official Facebook page, administered by: Caroline Collins, Janis Williams and Andy Ruffell. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

Those who are authorised to manage the account must ensure they abide by these guidelines at all times. Read in conjunction with Social Media Policy.

Where the above is not adhered to with staff it will be considered a breach of school's policies or procedures, as per section 4.

5.5 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited;
- Bandwidth usage;
- Email accounts;
- Telephone calls;
- User activity/access logs;
- Any other electronic communications.

Only authorised staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business;
- Investigate compliance with school policies, procedures and standards;
- Ensure effective school and ICT operation;
- Conduct training or quality control exercises;
- Prevent or detect crime;
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

6. Pupils

6.1 Access to ICT facilities

ICT facilities are available to pupils:

- Computers and equipment in school are available to pupils only under the supervision of staff;
- Specialist ICT equipment, such as that used for filming must only be used under the supervision of staff;
- Pupils will be provided with an individual login to access school systems.

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the Behaviour Policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright;
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination;
- Breaching the school's policies or procedures;
- Any illegal conduct, or statements which are deemed to be advocating illegal activity;
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate;
- Activity which defames or disparages the school, or risks bringing the school into disrepute;
- Sharing confidential information about the school, other pupils, or other members of the school community;
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel;
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities;
- Causing intentional damage to ICT facilities or materials;
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation;
- Using inappropriate or offensive language.

In addition to sanctions noted in the Behaviour Policy, school reserved the right to revoke a pupil's access to IT facilities.

7. Parents

7.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to sign the agreement in appendix 3 and adhere to the email protocol in appendix 2.

8. Data Security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

Pupils are allocated with a password to access the school system. Passwords are also allocated for all online learning including Reading Plus, Lexia and Times Tables Rockstars; pupils will have an individual password for each, this will be held by class teacher and the system administrators. Generic whole class passwords must not be used.

8.2 Software updates, firewalls, and anti-virus software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

Policy to be read in line with school's policy for data protection.

8.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the headteacher.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert headteacher or deputy head in their absence immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by One IT under direction of the headteacher.

9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **Proportionate**: OneIT uses systems to check that what it has in place is effective annually
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up to date:** with a system in place to monitor when the school needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up critical data is completed once a day and these backups are stored on a cloud-based backup systems that aren't connected to the school network and which can be stored off the school premises
- OneIT is delegated specific responsibility for maintaining the security of our management information system (MIS)
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with our LA to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

10. Internet Access

The school wireless internet connection is secured.

- Internet access at school is provided by One IT that affords a service designed for pupils. This includes a filtering system that is appropriate to the age of the pupils.
- Where the filter has not identified an inappropriate site, this must be reported to the headteacher or deputy head in their absence immediately. This will be reported to One IT.
- Access to appropriate information should be encouraged but internet access must be safe for all members of the school community from youngest pupil to teacher and administrative staff. Pupils will generally need protected access to the internet. The technical strategies to restrict access to inappropriate material fall into several overlapping types (sometimes all referred to as filtering):

    - Blocking strategies remove access to a list of unsuitable sites or newsgroups. Maintenance of the blocking list is a major task as new sites appear every day.
    - Filtering examines the content of web pages or e-mail messages for unsuitable words.
    - Blocking and/or filtering, as previously stated, is performed by the Internet Service Provider (ISP) and school is notified.
- The school will work in partnership with parents/carers, the LA, DFE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are effective in practice.
- If staff or pupils inadvertently discover unsuitable sites, the URL (address) and content will be reported to the Head Teacher who will notify One IT for an immediate response.
- Any material that the school suspects is illegal will be referred to One IT for blocking and further investigation.
- All school devices and assigned logins are set to access school internet connection.
- A guest login to the internet is available to visitors on request, oversight of this is maintained by the headteacher.

10.1 Pupils

- Pupils will be informed that internet use will be supervised and monitored.
- The purpose of internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems. Access to the internet is a necessary tool for staff and pupils. It is an entitlement for pupils who show a responsible and mature approach.
- Pupils in school are unlikely to see inappropriate content in books due to selection by publishers and teachers. This level of control is not so straightforward with Internet-based materials. Therefore, teaching should be widened to incorporate internet content issues, for instance the value and credibility of Web materials in relationship to other media. The tendency to use the Web when better information may be obtained from books will need to be challenged.
- Pupils will be taught ways to validate information before accepting that it is necessarily true.
- Pupils will be taught to acknowledge the source of information and observe copyright when using internet material for their own use.
- Pupils will be made aware that the writer of an e-mail or the author of a Web page might not be the person claimed.
- Pupils will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

The authorisation of internet access In school, all staff and all pupils will be granted access to the internet as a general requirement, with a single central written record maintained of pupils and staff who have access to the school internet connection. Parental permission will be required before children can access the Internet and an e-mail account.

- At Key Stage 1, the majority of the access to the internet will be by teacher or adult demonstration. However, there may be situations when children have supervised access to specific approved on-line materials.
- At Key Stage 2, internet access will be granted to a whole class as part of the scheme of work, after a suitable education in the responsible use of the Internet.
- Parents/carers will be informed that pupils will be provided with supervised internet access.
- Parents/carers will be asked to sign and return a permission form.

- Pupils must also, along with parents/carers, sign the letter sent home. This will be an indication by the parents/carers and pupils that they have discussed, understood and accept the implications of the use of the Internet in school and at home.

9.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA);
- Visitors need to access the school's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan).

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Website

Ingleby Mill currently has a web site that helps to celebrate pupils' work and promote the school. The Web site must reflect the school's ethos and that information is accurate and well-presented. As the school's web site can be accessed by anyone on the internet, the security of staff and pupils must be considered carefully. The publishing of pupils' full names beside photographs that identify individuals is considered inappropriate on web pages.

- The Headteacher will delegate editorial responsibility to a key member of staff with responsibility for this aspect of learning to ensure that content is accurate and quality of presentation is maintained.
- Staff will be made aware that the content of the work published on the Web needs to reflect the diversity of the audience.
- All material must be the author's own work, or where permission to reproduce has been obtained, clearly marked with the copyright owner's name.
- The point of contact on the web site should be the school address and telephone number. Home information or individual e-mail identities will not be published.
- Photographs must not identify individual pupils. Group shots or pictures taken over the shoulder will be used in preference to individual 'passport' style images.
- Actual names will not be used anywhere on the web site, particularly alongside photographs.
- Written permission from parents/carers will be sought by the signing of the 'Acceptable Use Policy' related to the use of the internet.

12. Monitoring and Review

The headteacher, deputy head and One It monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed annually to reflect the changing nature of school direction in relation to IT.

The governing body is responsible for approving this policy, the Safeguarding Governor will maintain oversight of this policy and its implementation.

13. Related Policies

All policies will be available for staff to access on Teams, governors will receive all policy documents via email. Parents can access all policies relevant to them on the school website, paper copies will be provided on request.

Relevant policies that should be read in conjunction with the Acceptable User Agreement:

- Social Media Policy
- Child Protection
- Behaviour
- Staff Discipline
- Data Protection
- Mobile Phone Use Policy
- Remote Learning

Appendix 1: Facebook Advice

10 rules for school staff on Facebook

1. Do not accept friends requests from pupils.
2. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead.
3. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional.
4. Check your privacy settings regularly.
5. Be careful about tagging other staff members in images or posts.
6. Don't share anything publicly that you wouldn't be just as happy showing your pupils.
7. Don't use social media sites during school hours.
8. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there.
9. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event).
10. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information.
11. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils).

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A pupil adds you on social media – to be read in line with the Social Media Policy

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening and log the incident on CPOMs

A parent adds you on social media

This is to be read in conjunction with the Social Media Policy. This should be treated as for pupil requests.

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Ingleby Mill Primary School

Acceptable use of the internet: agreement for parents and carers

Name of parent/carer:

Name of child:

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses the following channels:

- Email/text groups for parents (for school announcements and information)
- Our virtual learning platform
- Our official Facebook page

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, the School's Facebook group, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way
- Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers

Signed:	**Date:**

Appendix 3: Acceptable use agreement for pupils

Ingleby Mill Primary School

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

Name of pupil:

When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Share my password with others or log in using someone else's name or password
- Bully other people

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

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 using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors

Ingleby Mill Primary School

Acceptable use of the school's ICT facilities and internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) or deputy in their absence and let them know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**