At Chellaston Infant School, we believe that everyone should reach their full potential in a safe, fun and happy environment which promotes independence, self-worth and excellence. Everyone is a learner whose values are respected.

Chellaston Infant School
School Lane, Chellaston
DERBY, DE73 6TA
Telephone: 01332 700298

Email: admin@chellastoni.derby.sch.uk
Website: www.chellastoninfants.co.uk

Headteacher: Lindsay Galley

ONLINE SAFETY AND ACCEPTABLE USE POLICY

Date	Change made where?	Change description	Approved by Governors	Next review
18.10.21	New policy to better reflect new Computing scheme or work and safeguarding practices in school.		**Autumn 1 2021**	**Autumn 1 2022**
19.09.22	Policy renamed.	Online safety policy merged with the acceptable use policy. Section	26.09.22	Autumn 1 2023
19.09.22	Roles and responsibilities	Updated list to include ATOM IT.	26.09.22	Autumn 2 2023
19.09.22	The Four C's	Added section of the Four C's from the Keeping Children Safe in Education 2022 guidance.	26.09.22	Autumn 2023

Contents

Introduction 4
The Four C's 4
Legislation and guidance 4
Roles and responsibilities 5
Lindsay Galley – Headteacher and Designated Safeguarding Lead 5
ATOM IT - ICT manager 5
Joseph Jeffery – Computing Lead 5
All staff and volunteers 6
The Governing Board 6
Parents 6
Visitors and members of the community 6
Educating pupils about online safety 7
Educating parents about online safety 10
Cyber-bullying 10
Definition 10
Preventing and addressing cyber-bullying 10
Training 10
COVID-19 and home learning 11
Acceptable use of the internet in school 11
Unacceptable use 11
Exceptions from unacceptable use 12
Sanctions 12
Staff (including governors, volunteers, and contractors) 12
Access to school ICT facilities and materials 12
Use of mobile devices 13
Use of phones and email 13
Use of personal devices by Trainee Teachers 13
Personal use 13
Personal social media accounts 14
School social media accounts 14
Pupils 14
Access to ICT facilities 14
Search and deletion 14

Unacceptable use of ICT and the internet outside of school 14
Parents 15
Access to ICT facilities and materials 15
Communicating with or about the school online 15
The loan of school equipment to parents 15
Data security 15
Passwords 15
Software updates, firewalls, and anti-virus software 15
Data protection 15
Access to facilities and materials 16
Encryption 16
Internet access 16
Pupils 16
Member of the Local Governing Board, Parents and visitors 16
Staff using work devices outside school 16
Photographs 16
Social Media 17
How the school will respond to issues of misuse 17
Links with other policies 17
Useful Links and Resources 17

Introduction

The amount of people connected to the internet is increasing daily (South West Grid for Learning SWGfL). Technology is advancing and providing an ever-increasing range of methods to access the internet. At Chellaston Infant School we recognise the increasing prominence of technology and the internet in daily life. We endeavour to empower our pupils to be confident users of technology and the internet, being able to identify ways to be safe online and who they can talk to if they have any concerns or worries. To enable this, we aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The Four C's

As a whole school community, we all take responsibility for online safety and understand The Four C's: Content, Contact, Conduct and Commerce. The Four C's are used to classify the breadth of issues faced concerning online safety and are defined in the Keeping Children Safe in Education 2022 guidance (paragraph 136, page 35):

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Legislation and guidance

This policy is underpinned by the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships education and health education

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

This policy also complies and links to the EMET Employee Code of Conduct with regards to photography and social media.

Roles and responsibilities

Online Safety Leaders in school:

- Lindsay Galley: Designated Safeguarding Lead
- Lynn Hateley: Deputy Designated Safeguarding Lead
- Rachel Leyland: Deputy Designated Safeguarding Lead
- Kelly Leader: Learning Mentor & member of the Safeguarding Team
- Joseph Jeffery: Computing Lead
- Paul Stevenson: Safeguarding Lead Governor
- ATOM IT: IT support team employed by EMET

Lindsay Galley – Headteacher and Designated Safeguarding Lead

Lindsay Galley is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school, as underpinned by the Keeping Children Safe in Education guidance. The headteacher/DSL will be alerted to any Online Safety concerns logged through CPOMS along with the school's safeguarding team.

The Headteacher/DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged through CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and providing staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the governing board and computing lead to enable any concerns to be taught in online safety lessons

This list is not intended to be exhaustive.

ATOM IT - ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems (see Appropriate Monitoring and Filtering Procedures), which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems frequently
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

Joseph Jeffery – Computing Lead

- Ensure that online safety lessons are planned and delivered across school
- Ensure that staff are confident with their online safety subject knowledge and provide CPD with the headteacher
- Ensure that any concerns with technology used in school are reported to the ICT manager to be swiftly resolved

- Updating the Online Safety and Acceptable Use policy and Appropriate Monitoring and Filtering policy with the headteacher to reflect the computing curriculum and changes in government policy/guidance.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently.
- Class based staff to teach online safety lessons.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2).
- Class staff to produce an acceptable use policy with the children at the start of each academic year to provide ownership and understanding for pupils.
- Working with the DSL to ensure that any online safety incidents are logged through CPOMS and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs on CPOMS as provided by the designated safeguarding lead (DSL).

The governors responsible for safeguarding will also oversee online safety.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2).

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure the Acceptable Use Policy has been read and agreed

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

Educating pupils about online safety

The teaching of online safety is a paramount aspect of our computing curriculum. We use the Project Evolve: Education for a Connected World. Online safety lessons are taught every term, starting with each class creating an acceptable use policy that each pupil will receive a copy of for their work folders. The strands taught through the scheme are:

- Online bullying
- Online relationships
- Copyright and ownership
- Self-image and identity
- Privacy and security
- Managing online information
- Online reputation
- Health, well-being and lifestyle

The online safety scheme links to the following National Curriculum objectives:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

The teaching of online safety is a cross-curricular subject, with staff making links where appropriate to other subjects in the school curriculum.

Through online safety lessons and assemblies, staff will raise pupils' awareness of the dangers that can be encountered online by teaching the children how to be safe online. The school celebrate online safety events, such as Safer Internet Day and Anti-Bullying Week to promote online safety. Staff adapt teaching to current online safety issues such as new applications or software the children may access inside or outside of school.

Some of the key vocabulary that the children will learn and use are:

- Share
- Personal information
- Online safety
- Private/privacy
- Online
- Data
- Identity
- Reputation
- Online bullying
- Copyright
- Social media

	Aut 1	Aut 2	Spring 1	Spring 2	Summer 1	Summer 2
FS	Technology All Around Us: Introduction to using the devices in school. Online Safety Create an Acceptable Use Policy in each class.	Programming – sequencing using unplugged activities Link to debugging Online Safety Online bullying	Digital Creators: Using Draw and Tell app to create a picture and record what they have made. Online Safety Online relationships	Digital Creators: Online Safety Copyright and ownership	Programming – sequencing using unplugged activities Link to debugging Online Safety Self-image and identity	Opportunities to practise any skills the children have found tricky/not yet covered. Online Safety Privacy and security Managing online information
Y1	Technology All Around Us: Parts of a computer. What this looks like in real world Online Safety Create an Acceptable Use Policy in each class.	Programming – understanding and creating algorithms unplugged and beebot activities. Link to debugging Online Safety Online bullying	Digital Creators: Digital art – using iPad to create and edit a picture Online Safety Online relationships	Data handling: Using websites and apps to sort and classify objects by their properties Online Safety Copyright and ownership	Programming with Scratch Jr. Exploring the app and the different elements. Online Safety Self-image and identity	Opportunities to practise any skills the children have found tricky/not yet covered. Online Safety Privacy and security Managing online information
Y2	Technology All Around Us: Parts of a computer – understanding how they work What this looks like in real world Online Safety Create an Acceptable Use Policy in each class.	Programming – Scratch Jr Link to debugging Online Safety Online bullying	Digital Creators: Stop Motion Animation Online Safety Online relationships	Data handling Using Purple Mash to create pictograms. Databases Online Safety Copyright and ownership	Programming with Scratch Jr. Designing and programming. Online Safety Self-image and identity	Opportunities to practise any skills the children have found tricky/not yet covered. Online Safety Privacy and security Managing online information

This is our long term plan for computing. The green strands are the online safety aspects of the computing curriculum. Online Reputation and Health, Well-being and Lifestyle strands from the scheme will be delivered through school assemblies.

Online Safety Overview Project Evolve – Educated for a Connected World			
	Foundation Stage	Year 1	Year 2
Self-image and identity	In this strand children will learn how to say no to people when online and in real life using different scenarios and discuss what the appropriate thing to do is.	In year 1 children will learn how to recognise how people may be feeling online and who to talk to if they are worried about being online.	In year 2 children will learn how people may act differently online and offline and learn some different issues people may encounter that may make them sad or upset.
Online relationships	In FS2 the children will begin to understand how the internet can be used to communicate with other people.	In year 1 children will learn the importance of asking for permission before accessing the internet. Children will discuss examples of how they have used the internet to connect with others such as video calls. They will learn the importance of kindness to others when communicating online.	In year 2 the children will develop their understanding of asking for permission before agreeing/doing something online by asking a trusted adult. Children will be able to identify who their trusted adults are at home and in school.
Online reputation	Children will begin to learn how information can be put online.	Children in year 1 will learn that information put online can stay there for a long time and be copied by other people. Children will develop their understanding of what information is safe for them to put online and the necessity for them to check with a trusted adult first.	The children will learn about their digital footprint and how information that is put on the internet is very hard to permanently remove. They will learn that information that they put online can be viewed by other people.
Online bullying	Children will learn how people can be unkind online and be able to explain how this might make people feel.	In year 1 children will explore how to behave online so that they do not upset other people.	Children will learn to explain what online bullying is, that anyone who experiences bullying is not to blame and how and who to go to for help if being bullied online.
Managing online information	Children will begin to learn how the internet can be used as a source to find information. Children will discuss the different devices that they could use to access the internet.	Children will learn the different ways that they can use tools to search for information on the web. They will learn that not everything that they read or see on the internet is real and what to do if they see something that upsets or worries them online.	Children will learn how to search for information with key words, how to navigate a webpage, understand what voice activated searching is and understand that not everything on the internet is true.
Health, well-being and lifestyle	Children will learn how to be safe and healthy when using technology at home and beyond home.	The children will learn to express how to be safe when using technology at home or beyond home.	The children will learn how to explain the rules and guidance for using different technology in school, home and public places and how these rules help people accessing online technologies.
Privacy and security	Children will begin to understand what information is personal and who are trusted people that information can be shared with.	Children will learn about the importance of passwords and the information that is personal to ourselves. They will learn of the importance to ask a trusted adult before sharing information online.	Children will continue to learn about passwords, what keeping information private means, be able to explain how they can keep their information private and understand what devices are connected to the internet in their homes.
Copyright and ownership	Children will begin to understand that the work they create belongs to them.	Children will develop their understanding that the work they create belongs to them and that things other people have created do not belong to them.	Children will continue to develop their understanding that work produced by them belongs to them and that things created by others does not belong to them.

This is the long term overview of our online safety curriculum that follows the Education for a Connected World scheme.

Educating parents about online safety

The school will raise parents' awareness of online safety in newsletters and in information via our website or Class Dojo. This policy will also be shared with parents via the school website. Training from external trainers have previously been offered for parents and carers.

Online safety will also be covered during parents' evenings as appropriate.

If parents have any queries or concerns in relation to online safety, these can be raised to any member of staff who will ensure that the headteacher and the safeguarding team are informed.

Concerns or queries about this policy can be raised with any member of staff who will inform the headteacher and the computing lead.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. This will be more specifically taught through the Online Bullying strand of the Project Evolve: Education for a Connected World scheme.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also provides information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, briefings and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Staff teaching online safety lessons will have training to ensure lessons are taught effectively, which will be monitored through learning walks, observations and planning/work scrutinies. Staff will regularly complete a skills audit for online safety that can be used by the computing lead and headteacher to plan and provide CPD where necessary (appendix 4).

Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and safeguarding policy.

COVID-19 and home learning

Due to COVID-19 learning has occurred from home for many children during past few academic years. Staff have provided resources and activities for parents and carers to use for home learning. All websites and resources provided are rigorously checked by staff before being shared to ensure that there is no inappropriate content that the children may access. Photos uploaded onto the children's portfolios on Class Dojo were approved by staff to ensure that content is appropriate.

In the current 2022-2023 academic year, home learning will be provided if there is a partial or full school closure. Home learning will be posted onto the school website and a link will be shared with parents when necessary. Class Dojo will continue to be used as a method of communication between staff and parents/pupils. Loom has also been used by staff to provide educational videos to support the curriculum content provided through home learning. Videos are checked by staff to ensure that all content is appropriate for children to watch at home.

Children will be given the opportunity for daily contact with staff through submitting work onto their Class Dojo portfolios which is acknowledged and feedback given by class staff. When delivering video assemblies or teaching with Zoom and/or Loom, staff will ensure that they are in a suitable environment while using any webcam to ensure secure and safe broadcasts. Any non-engagement with home learning will initially be followed up by the class teacher through a supportive conversation with parents or carers. SLT will provide further support if necessary.

We will:

- Check parents and carers access to the internet, devices and the number of these at home etc. along with their comments on the home learning when appropriate.
- Remind parents of the risks of using online resources and provide support and resources where appropriate to keep the children safe.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1, 2 and 3)

Pupils will create an acceptable use policy with their class teachers each year in Autumn 1 that is referred to throughout the year when appropriate (appendix 1).

Visitors will be expected to read and agree to the school's terms on ICT and Internet acceptable use as established in this policy if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

When using email or electronic communications involving pupil information, staff will use initials or first names only to ensure that personal information is protected.

More information is set out in the acceptable use agreements in the appendices.

Breaches of acceptable use may be dealt with under our Staff Disciplinary policy, School Behaviour Policy and Staff Code of Conduct.

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.

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

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.

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. Applications for such use will need to be in writing and will be considered at Executive level before a decision is made, the decision will be communicated in writing.

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 School Behaviour, Staff Discipline and Staff Code of Conduct.

Staff (including governors, volunteers, and contractors)

Access to school ICT facilities and materials

The school's IT support team manages access to the school's ICT facilities and materials for school staff. 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 that they must use when accessing the school's ICT facilities. Passwords must be updated every 90 days.

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 school's IT support team via ATOM IT.

Use of mobile devices

Each class is provided with a tablet in order to access the secure parent platform Class Dojo along with the FFT (Fischer Family Trust) EYFS Assessment Tracker. Photographs uploaded onto these platforms should only be taken using a school mobile device, and mobile device galleries regularly deleted and not used for the storage of images.

Parental permission is sought for the use of any image of a child at the point of admission to school.

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.

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. Emails sent via 'Egress' should be used for this purpose.

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 School IT team, the Headteacher and the Data Protection Officer (DPO) immediately and follow our 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.

Use of personal devices by Trainee Teachers

Trainee Teachers and other long term work experience students must discuss the personal use of their own IT equipment such as laptops with the Headteacher.

Personal laptops or tablets must only be used for the purposes of planning and assessment within a PPA situation and not with children present. Any work where a laptop is required in class the Trainee Teacher or student must use the class-based IT equipment such as teachers' laptop, TA laptop, a pupil laptop or tablet.

The use of personal mobile phones or tablets is not permitted in class.

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 School IT team 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 pupil contact 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. Where breaches of this policy are found, disciplinary action may be taken.

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) and use of email to protect themselves online and avoid compromising their professional integrity.

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.

The school has guidelines for staff on appropriate security settings for social mediaaccounts (see appendix).

School social media accounts

The school has an official Facebook and Twitter page, managed by The Headteacher. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The school social media accounts should only be used to promote positive school activity, that of the school PTFA, any EMET or other community groups activity which may be relevant to, or of interest to, Chellaston Infant School parents.

Pupils

Access to ICT facilities

- Computers and equipment in the school's classrooms are available to pupils only under the supervision of staff
- Specialist ICT equipment, such as that used for music or design and technology must only be used under the supervision of staff.

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.

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

Parents

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.

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. Appropriate use is shared in our school prospectus.

The loan of school equipment to parents

Devices such as laptops that parents may borrow to facilitate remote learning are installed with appropriate safeguards to ensure online safety of pupils. Parents will sign an Acceptable Use agreement before borrowing IT equipment from school.

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.

Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. These password must be changed every 90 days. 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.

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.

Data protection

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

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 ATOM IT.

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 the Headteacher 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.

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 the School IT team.

Internet access

The school wireless internet connection is secured. Details of the Monitoring and Filtering processes can be found in our Monitoring & Filtering Policy.

Pupils

Pupils do not bring their own devices to school and therefore do not have internet access unless accessing the internet via a school PC or tablet.

Member of the Local Governing Board, 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.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff have their own login details that they can use. School tablets are also password protected. Staff must not share their passwords with anyone not authorised to use the school devices. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted. If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set in the ICT and Internet Acceptable Use Policy. Personal use of ICT facilities must not be overused or abused. The School IT team may withdraw permission for it at any time or restrict access at their discretion.

Photographs

Taken from the EMET Employee Code of Conduct:

If there is a requirement in the member of staff's role to take photographs of children for school purposes this must be carried out using school equipment. Any photographs taken in school remain the property of the school and will only be used for official school business such as displays, the

school web site or newsletters. No images taken within the school premises should be published unofficially by individuals on social media or other such forums.

Social Media

Taken from the EMET Employee Code of Conduct:

Staff should be extremely cautious when using social media or networking sites outside of work and avoid publishing, or allowing to be published, any material, including comments or images that could damage their professional reputation and/or bring their school or the Trust into disrepute. Where staff do use social media or networking sites, profiles should be set as 'private' and under no circumstances should staff allow access to pupils, their families or carers.

Staff and governors should be mindful that requirements in relation to maintaining the confidentiality of pupils, their families, colleagues and any matters relating to the school itself apply to all forms of communication, including social media and networking sites.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. If appropriate, staff will log any concerns on CPOMS so that the safeguarding team is aware of the issue, as well as the computing lead if the issue involves resources used for computing and online safety lessons.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Appropriate Monitoring and Filtering Procedures

Useful Links and Resources

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- https://www.childnet.com/parents-and-carers/hot-topics
- Parent resources document - https://www.childnet.com/resources/parents-and-carers-resource-sheet
- This website reviews different games/apps and their safety features and risks https://www.net-aware.org.uk/
- Our school online safety webpage https://www.chellastoni.derby.sch.uk/about-us/online-safety/
- National Online Safety Website - https://nationalonlinesafety.com/

- Keeping Children Safe in Education - https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
- Teaching Online Safety in Schools - https://www.gov.uk/government/publications/teaching-online-safety-in-schools
- Think U Know – online safety resources for children - https://www.thinkuknow.co.uk/professionals/
- Education for a Connected World - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896323/UKCIS_Education_for_a_Connected_World_.pdf

13. Appendix

Appendix 1 – Acceptable Use Policy - class/children

Appendix 2 – Acceptable Use Policy – Staff, Governors, Volunteers and Visitors

Appendix 3 – Acceptable Use Policy – Parents and Carers

Appendix 4 – Online Safety Staff Training Needs Audit

Appendix 5 – Facebook and Social Media Cheat Sheet

Appendix 1

Acceptable Use Policy – Class/Children

Keeping Safe Online and Computing Rules

By Class

This is how we stay safe when we are using computers:

Written and agreed by Class

Appendix 2

Acceptable Use Policy – Staff, Governors, Volunteers and Visitors

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), 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 • Take photographs of pupils without checking with teachers first • 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 will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree 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) know if a pupil informs me they have found any material which might upset, distress or harm them or others via CPOMS, 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:**

Appendix 3

Acceptable Use Policy – parents and carers

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PARENTS/CARERS	
Name of Parent/carers:	
When I use any ICT systems for working/communication with school: • Use content shared on Class Dojo and the school website appropriately. • Keep photos shared on Class Dojo and the school website private and not share them on social media. • Keep any passwords for accounts for websites provided by school private. • Communicate in an appropriate and respectful manner. • Ensure any concerns regarding online safety are shared with the school. • Ensure any content shared via school communication systems (e.g. Class Dojo, email) is appropriate and safe. • Use social media respectfully in relation to school, share any concerns with staff. • I will not use any devices to record or photograph children at school events.	
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 working and communicating with the school's ICT systems	
Signed (parent/carer):	**Date:**

Appendix 4

Online Safety Training Needs Audit

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for parents?	
Are you familiar with the school's acceptable use agreement for children?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5

Facebook and Social Media Cheat Sheet

Don't accept friend requests from pupils on social media

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. 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)
9. 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
10. 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

- 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

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

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