



# ICT, internet and electronic communication acceptable use policy

**Designated Safeguarding Lead (s): Karen Burton, Headteacher / Tina Arckless, Pastoral care.**

<b>Link Governor for Safeguarding</b>	R Raynor
<b>Link Governor for Computing</b>	Mrs K Peace
<b>Computing Lead and technical support</b>	Danielle Hamilton / Esteem ICT manager - Adrian Foster

**Approved by:** K.Burton **Date:** Sept 2023

**Last reviewed on:** September 2023

**Next review due by:** September 2024

© The Key Support Services Ltd | For terms of use, visit [thekeysupport.com/terms](https://thekeysupport.com/terms)

## Contents

1. Introduction and aims .....	3
2. Relevant legislation and guidance .....	3
3. Definitions .....	3
4. Unacceptable use .....	4
5. Staff (including governors, volunteers and visitors).....	5
6. Pupils .....	9
7. Parents .....	11
8. Data security .....	11
9. Protection from cyber attacks .....	12
10. Internet access .....	13
11. Monitoring and review.....	14
12. Related policies .....	14
Appendix 1: Facebook cheat sheet for staff.....	15
Appendix 2: Acceptable use of the internet: agreement for parents and carers .....	17
Appendix 3: Acceptable use agreement for EARLY YEARS and YEAR 1 .....	18
Appendix 4: Acceptable use agreement for YEAR 2 .....	20
Appendix 5: Acceptable use agreement for learners with SEND.....	22
Appendix 6: Acceptable use agreement for staff, governors, volunteers and visitors .....	24
Appendix 7: Cyber security glossary.....	26

---

## 1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including senior leadership teams), 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 behaviour policy/staff code of conduct.

## 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 \(KSIE 2023\)](#)
- › [Searching, screening and confiscation: advice for schools](#)
- › [National Cyber Security Centre \(NCSC\)](#)
- › [Education and Training \(Welfare of Children Act\) 2021](#)

## 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

See appendix 6 for a glossary of cyber security terminology.

## 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
- › Online gambling, inappropriate advertising, phishing and/or financial scams
- › Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- › Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- › 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
- › Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher or any other relevant member of staff 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 (on the school premises and/or remotely) 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.

## 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 behaviour/staff code of conduct. The police may also be contacted.

# 5. Staff (including governors, volunteers, and visitors)

## 5.1 Access to school ICT facilities and materials

The school's ICT Team manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- › Computers, tablets, mobile phones 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.

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 Computing Lead in the first instance.

Visitors are required to confirm they have read and agree to safeguarding procedures/mobile phone use on entry to the building via the electronic sign in screen.

### 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.

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 or password protected 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 that contains the personal information of another person, they must inform the Headteacher 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.

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

Elmsleigh Infant and Nursery School recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

Staff choose to access school information from their own devices. Any member of staff wishing to do this must be aware that they have a direct personal responsibility for ensuring that the device they choose to use has the benefit of encryption, that is above and beyond simple password protection. Staff must ensure that personal devices such as mobile smart phones, tablets and other portable electronic equipment are set to lock and only open with encrypted passcodes to prevent unauthorised access.

School will support and enable staff to ensure that their devices are compliant. **If any member of staff uses a device without these safeguards in place it will be a disciplinary breach if data is unlawfully accessed by a third party.**

### Staff MUST:

- **Keep mobile phones and personal devices in a safe and secure place during lesson times.**
- **Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.**
- **Not use personal devices during teaching periods / when in contact with children unless permission has been given by the Headteacher, except in emergency circumstances.**
- **Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.**

Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers, except in cases of emergency. Any pre-existing relationships, which could undermine this, will be discussed with the Headteacher.

### Staff will not use personal devices:

- **To take photos or videos of learners and will only use work-provided equipment for this purpose, unless authorised by the headteacher, for specific purposes.**
- **Directly with learners and will only use work-provided equipment during lessons/educational activities.**

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 Computing Lead / 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 time / class 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 (see section 5.5). 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 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

### **5.2.1 Personal social media accounts**

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.

This policy clarifies that online conduct is the employee's responsibility, and it is important that staff are aware that posting information on social networking sites cannot be isolated from their working life.

Any information published online can be accessed around the world within seconds and will be publicly available for all to see and is not easy to delete/withdraw once published. Elmsleigh School views any comment that is made on a social media site as made publicly, and that any inappropriate comment made, will be considered in the context of which it is made. Staff are advised to be mindful that nothing on a social media site is 'private' so comments made must still meet the standards of the Staff Code of Conduct and other relevant policies.

Staff may be accountable for actions outside of work, including making comments on social media sites, if that is contrary to any of School's policies, impacts on or compromises the employee's ability to undertake their role, or undermines management decisions. Such behaviour would be investigated and may result in disciplinary action being taken, and ultimately could result in dismissal.

The Headteacher and Governors will give consideration, when reaching decisions relating to potential disciplinary cases for breach of such a code, to the difficulty of staff members in 'controlling their image' all the time, and that manipulation by others is extremely easy. The Head/Governors will consider whether the 'image' had been created voluntarily by the member of staff.

Staff are reminded that, as a safeguarding issue, they should always be careful about who they are 'talking to'. It is very easy to hide an identity in an on-line conversation.

Elmsleigh School views any comment that is made on social media to, potentially, have been made publicly. However, any inappropriate comment will be considered in the context in which it is made. Members of staff should inform the Headteacher if they consider any content shared on a social media site potentially conflicts with their role.

Staff should be aware that all comments made through social media must meet the standards of the relevant legislation and regulations, including data protection legislation (GDPR 2018) and the expectations of staff conduct as expressed in the school's policies.

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

Staff are not allowed to access social media websites for personal use from the school's computers or devices. Leaving social media sites 'running' constantly in work's time is considered to be a breach of the acceptable use of this policy, and would be considered to be using school resources for personal use, in work's time, and such would be investigated under the Disciplinary procedure. These provisions also apply to personal computers and mobile devices.

## **5.3 Remote access**

We allow staff to access the school's ICT facilities and materials remotely. This is through the use of Office 365 and the Cloud – One Drive.

- Who manages it? – The One Drive and Office 365 is managed by the ICT Team.
- Security arrangements – All staff have individual passwords, and any access can be monitored.

- › Protocols for remote access –Staff may access the OneDrive through their school laptop or their emails through office 365.
- › 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 required 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.

## 5.4 School social media accounts

Elmsleigh Infant and Nursery School official social media channels are: Facebook pages - ‘Elmsleigh Infant and Nursery School’ official group page and ‘Friends of Elmsleigh’ Fundraising group.

The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes. The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher. Leadership and selected staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence:

- Karen Burton (Headteacher)
- Ellen Collins (Deputy head)
- Laura Mansfield (Assistant Head)
- Ruth Samme (School Business Manager)
- Elisha Flamson (Communications and Office Co-ordinator)
- Danielle Hamilton (Computing Lead)

Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.

Staff use setting provided email addresses to register for and manage any official social media channels.

Official social media sites are suitably protected and linked to our website.

All communication on official social media platforms will be clear, transparent and open to scrutiny.

Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.

Any official social media activity involving learners will be moderated possible.

Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.

We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

There should be no expectation that either staff or pupils will be available outside normal school hours. If schools are to utilise this, Headteachers should ensure that a reasonable level of monitoring is in place, to prevent any inappropriate comments or ‘cyber-bullying’, and ensure that pupils know that such monitoring is taking place.

## 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 ICT 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

## 5.6 Copyright

Employees may be in violation of copyright law if text is simply cut and pasted into another document. This may equally apply to photographs and music samples used as illustration or backing track in resource materials. Teachers should make it clear to pupils that care should be taken when including this type of material in any school or exam work. Most sites contain a copyright notice detailing how material may be used. If in any doubt about downloading and using material for official purposes, legal advice should be obtained. Unless otherwise stated on the site all down loaded material must be for curricular or research purposes and must not be passed to third parties.

Downloading of video, music files, games, software files and other computer programs – for non-work related purposes-is not allowed. These types of files consume large quantities of storage space on the system and may violate copyright laws.

## 5.7 Dojo

*ClassDojo is a school communication platform that connects teachers, students, and families, and brings them closer together. This is done in two ways. One, by sharing what's being learned in the classroom back home through portfolios, photos, videos, and messages. And, two, by helping students build social-emotional skills through in-classroom feedback and engaging activities. These relationships require trust, which is why we've made sure ClassDojo is a safe and private environment for teachers, parents, and students. – Class Dojo*

**(<https://static.classdojo.com/docs/ClassDojoTeacherCommonQuestionsPrivacyPolicies.pdf>)**

As a school, class teachers use Class Dojo to communicate with parents. This is an online platform which enables the sharing of photographs, videos, work and also includes a messaging service.

All parents are provided with their own unique log-in which enables them to see the class page and their child's profile. Class Dojo is GDPR compliant and only the student themselves, their families, and their connected teachers or school leaders can see a student's profile and portfolio.

Permission is gained from parents before pictures/videos are shared. Further information can be obtained from <https://www.classdojo.com/privacycenter/>

## 6. Pupils

## 6.1 Access to ICT facilities

- › Computers and equipment 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
- › Pupils will be provided with an account linked to PurpleMash, which they can access from any device by using the following URL <https://www.purplemash.com/sch/elmsleigh>
- › Pupils will be provided with a personal log in for the following online platforms - Dojo.

## 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.

Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

## 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
- › Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- › 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

Children are provided with acceptable use agreements which are sent home for parents to discuss/sign with them as well as discussion in school. (See appendix 3/4/5)

## 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 2.

## 8. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore 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.

All staff will use a password manager to help them store their passwords securely. Teachers will generate passwords for pupils using a password manager/generator and keep these in a secure location in case pupils lose or forget their passwords.

Passwords for Office 365, Integris and other online platforms will generate regular password update prompts.

### 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.

## 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 ICT Team (Esteem ICT Team, Computing Lead and Business manager)

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.

## 8.5 Encryption

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

School staff may only use personal devices 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.

## 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'**: the school will verify this using a third-party audit to objectively test that what it has in place is up to scratch.
  - **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 up to scratch and secure as they can be
- › Back up critical data and store these backups on cloud based systems
- › Delegate specific responsibility for maintaining the security of our management information system (MIS) to our Esteem ICT Team
- › 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 seeing if they have the [Cyber Essentials](#) certification
- Develop, review and test an incident response plan with the IT department, for example, including how the school will communicate with everyone if communications go down, who will be contacted when, and who will notify [Action Fraud](#) of the incident. This will be reviewed and tested annually and after a significant event has occurred, using the NCSC's '[Exercise in a Box](#)'
- Work with our Trust 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.

- Our ISP is Primary ICT – this is used across the Esteem Trust.
- We use 'Securly' for our filtering system (<https://www.securly.com/filter>) which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the [Internet Watch Foundation](#) (IWF) list.
- We work with Securly to ensure that our filtering policy is continually reviewed.

If children discover unsuitable sites or images:

- Child to click on the 'Red Button' when using Chrome boxes or close the screen on a Chromebook and inform a member of staff immediately.
- The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or Online Safety lead.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Derbyshire Police or CEOP.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.
- Staff will receive yearly training on the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Pupils access the internet through the connected devices in school, under adult supervision. Pupils have access to our online learning platforms and other risk assessed websites.

### 10.2 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. Monitoring and review

The headteacher and Computing Lead monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year.

The governing board is responsible for approving this policy.

## 12. Related policies

This policy should be read alongside the school's policies on:

- Online safety
- Safeguarding and child protection
- Behaviour
- Professional protocol for Elmsleigh staff
- Data protection
- Remote learning
- Laptops for home learning
- Computing

## Appendix 1: Facebook cheat sheet for staff

### 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](https://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](https://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 to do 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



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

### Elmsleigh Infant and Nursery 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:

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

If attending a meeting via Zoom, I will ensure the household are aware of the meeting to maintain appropriate content and I will not record the video.

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 page, 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:**

## Elmsleigh Infant and Nursery School Acceptable Use of Technology Policy Acknowledgment - Early Years and Year 1

I, with my parents/carers, have read and understood the Acceptable Use of Technology Policy (AUP):

### When using a laptop, chromebook or ipad in school:

- I only use the internet when an adult is with me 
- I only click on links and buttons online when I know what they do 
- I keep my information about myself and passwords safe 
- I only send messages online which are polite and friendly 
- I know that Elmsleigh Infant and Nursery school can see what I am doing online 
- I always tell an adult/teacher/member of staff if something online makes me feel unhappy or worried 
- I know that if I do not follow the rules then I will not be able to use school technology and my parents will be told

I agree to follow these rules all of the time when I am using the internet at home or at school.

I, with my child, have read and discussed learner acceptable use of technology policy (AUP). I understand that the aim of the AUP is to help keep my child safe online and applies to the use of the internet and other related devices and services, inside and outside of the school/setting.

1. I am aware that any internet and IT use using school/setting equipment may be monitored for safety and security reasons to safeguard both my child and the school/setting systems. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.
2. I understand that the school/setting will take every reasonable precaution, including monitoring and filtering systems, to ensure my child will be safe when they use the internet and other associated technologies. I understand that the school/setting cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
3. I with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school/setting community.
4. I understand that the school/setting will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety.

5. I will inform the school/setting or other relevant organisations if I have concerns over my child's or other members of the school/setting communities' safety online.
6. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet both in and out of school.
7. I will support the online safety approaches and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

Child's Name..... Child's Signature .....

Class..... Date.....

Parents Name.....

Parents Signature..... Date.....

## Appendix 4: Acceptable use agreement for YEAR 2

### Elmsleigh Infant and Nursery School Acceptable Use of Technology Policy Acknowledgment – Year 2

I, with my parents/carers, have read and understood the Acceptable Use of Technology Policy (AUP):

**When using a laptop, chromebook or ipad in school:**

#### Safe

- I ask an adult if I want to use the internet
- I keep my information private on the internet
- I know that if I do not follow the rules then I will not be able to use school technology and my parents will be told



#### Meeting

- I tell an adult if I want to talk to people on the internet

#### Accepting

- I don't open messages from strangers
- I check web links to make sure they are safe

#### Reliable

- I make good choices on the internet
- I check the information I see online

#### Tell

- I use kind words on the internet
- If someone is mean online then I don't reply, I show the message to an adult
- If I see anything online that I don't like, I will tell an adult



(Based on Childnet's SMART Rules: [www.childnet.com](http://www.childnet.com))

I agree to follow these rules all of the time when I am using the internet at home or at school.

I, with my child, have read and discussed learner acceptable use of technology policy (AUP). I understand that the aim of the AUP is to help keep my child safe online and applies to the use of the internet and other related devices and services, inside and outside of the school/setting.

1. I am aware that any internet and IT use using school/setting equipment may be monitored for safety and security reasons to safeguard both my child and the school/setting systems. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.
2. I understand that the school/setting will take every reasonable precaution, including monitoring and filtering systems, to ensure my child will be safe when they use the internet and other associated technologies. I understand that the school/setting cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

3. I with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school/setting community.
4. I understand that the school/setting will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety.
5. I will inform the school/setting or other relevant organisations if I have concerns over my child's or other members of the school/setting communities' safety online.
6. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet both in and out of school.
7. I will support the online safety approaches and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

Child's Name..... Child's Signature .....

Class..... Date.....

Parents Name.....

Parents Signature..... Date.....

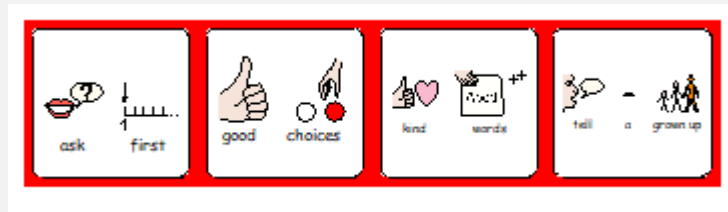
## Appendix 5: Acceptable use agreement for learners with SEND

### Elmsleigh Infant and Nursery School Acceptable Use of Technology Policy Acknowledgment – Learners with SEND

I, with my parents/carers, have read and understood the Acceptable Use of Technology Policy (AUP):

#### When using a laptop, chromebook or ipad in school:

- I ask a grown up if I want to use the computer
- I make good choices on the computer
- I use kind words on the internet
- If I see anything that I don't like online, I tell a grown up
- I know that if I do not follow the rules then I will not be able to use school technology and my parents will be told



I agree to follow these rules all of the time when I am using the internet at home or at school.

I, with my child, have read and discussed learner acceptable use of technology policy (AUP). I understand that the aim of the AUP is to help keep my child safe online and applies to the use of the internet and other related devices and services, inside and outside of the school/setting.

1. I am aware that any internet and IT use using school/setting equipment may be monitored for safety and security reasons to safeguard both my child and the school/setting systems. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.
2. I understand that the school/setting will take every reasonable precaution, including monitoring and filtering systems, to ensure my child will be safe when they use the internet and other associated technologies. I understand that the school/setting cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

3. I with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school/setting community.
4. I understand that the school/setting will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety.
5. I will inform the school/setting or other relevant organisations if I have concerns over my child's or other members of the school/setting communities' safety online.
6. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet both in and out of school.
7. I will support the online safety approaches and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

Child's Name..... Child's Signature .....

Class..... Date.....

Parents Name.....

Parents Signature..... Date.....

## Appendix 6: Acceptable use agreement for staff, governors, volunteers and visitors

### Acceptable use of the school's ICT facilities and the 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 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 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) and ICT manager 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:**



## ACCEPTABLE USE AGREEMENT SCHOOL EQUIPMENT & SOFTWARE – STAFF

Name: (please print):

Hardware Details	Serial Number / ID	Date issued
Laptop model -		
Visualiser		
Microsoft web-cam		Sept 2020
Desktop PC (classroom based)		
Camera Model -		
Teacher Ipad		
Classroom Projector		

Software Details	Additional info
Microsoft Windows 10	Automatically updates to latest version
Microsoft Office 365 / OneDrive	Automatically updates to latest version
Anti-Virus software – Windows Security	
Adobe reader	Checked monthly for latest version
Adobe flash player	Discontinues as of Dec 2020
Google Chrome	Automatically updates to latest version
Joinit c9	Cursive font for Microsoft word
SMART Notebook 11	
VLC media player	

### DECLARATION

I confirm that I have received the equipment and software as specified above and understand the terms and conditions of use as set out in the Acceptable Use Policy.

Signed:

Date:

## Appendix 7: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) [glossary](#).

TERM	DEFINITION
<b>Antivirus</b>	Software designed to detect, stop and remove malicious software and viruses.
<b>Cloud</b>	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
<b>Cyber attack</b>	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
<b>Cyber incident</b>	Where the security of your system or service has been breached.
<b>Cyber security</b>	The protection of your devices, services and networks (and the information they contain) from theft or damage.
<b>Download attack</b>	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
<b>Firewall</b>	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
<b>Hacker</b>	Someone with some computer skills who uses them to break into computers, systems and networks.
<b>Malware</b>	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
<b>Patching</b>	Updating firmware or software to improve security and/or enhance functionality.
<b>Pentest</b>	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
<b>Phishing</b>	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
<b>Ransomware</b>	Malicious software that stops you from using your data or systems until you make a payment.

TERM	DEFINITION
<b>Social engineering</b>	Manipulating people into giving information or carrying out specific actions that an attacker can use.
<b>Spear-phishing</b>	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
<b>Trojan</b>	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
<b>Two-factor/multi-factor authentication</b>	Using 2 or more different components to verify a user's identity.
<b>Virus</b>	Programs designed to self-replicate and infect legitimate software programs or systems.
<b>Virtual Private Network (VPN)</b>	An encrypted network which allows remote users to connect securely.
<b>Whaling</b>	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.