# ICT, Online Safety and Acceptable Use Policy

| | | | |
|---|---|---|---|
| Approved by | CEO | Date Approved | 29 August 2025 |
| Review cycle | Every 3 years | Date of next review | Spring 27 |

| Version | Author | Date | Changes |
|---|---|---|---|
| 1.0 | J Hawkins, COO and A Marsh, Trust DSL | 17/4/23 | Updated in line with KCSIE 2023. |
| 2.0 | A Marsh, Trust DSL | 01/07/24 | Reviewed in line with KCSIE 2024. Reduced wording for clarity where possible, added sentence to clarify data storage (8.3). Clarified roles and processes to reflect practice. Review cycle lengthened. |
| 2.1 | M Boddington | 28/05/25 | 3. Definitions – 4 Cs included<br>6.1 Added details on processes and online safety measures, including filters and monitoring on Trust networks to protect pupils, staff, and volunteers.<br>7.1 Data protection information updated |
| 2.2 | M Boddington | 15/07/25 | Introduction -Inclusion of a child-centred safeguarding statement in the policy introduction.<br>**3.Safeguarding Risks from Misinformation, Disinformation and Conspiracy Theories**<br>9 Clarification of the Designated Safeguarding Lead's (DSL) responsibilities for online safety, including training and monitoring.<br>5 Requirement for all staff to receive online safety training as part of induction and annually thereafter.<br>5 Clarification on staff reading requirements: Part One or Annex A of KCSIE 2025 depending on role.<br>5.5 Addition of guidance on recognising and responding to harmful sexual behaviour (HSB) and online child-on-child abuse.<br>5.5 New section addressing safeguarding considerations for gender questioning children.<br>7.2 Expanded guidance on the safe and ethical use of AI in education |

## Contents



---

This policy is underpinned by a child-centred approach to safeguarding, ensuring that the best interests of the child are always prioritised in the use of ICT and online systems.

## 1. Introduction and aims

ICT is a critical resource for our schools supporting teaching and learning, pastoral and administrative functions. However, the ICT resources and facilities our Trust uses also pose risks to data protection, online safety, and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of Trust ICT resources for staff, pupils, parents, and governors.
- Establish clear expectations for the way all members of our school communities engage online.
- Support our policy on data protection and safeguarding.
- Prevent disruption to the Trust through the misuse, or attempted misuse, of ICT systems.
- Support schools in teaching pupils safe and effective internet and ICT use.

All users must sign the acceptable use agreement relevant to them in the appendices of this document. Each school must keep an up-to-date record of users who have done this.

## 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
- Searching, screening and confiscation: advice for schools
- Working Together to Safeguard Children

## 3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, computers, 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 Trust 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 Trust 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.

**Online Safety** – a effective approach to online safety is helpful to protect and educate pupils, students and staff in their use of technology and enables mechanisms to identify, intervene and escalate concerns. There are four main areas of risk in schools:

- **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 non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

**Safeguarding Risks from Misinformation, Disinformation and Conspiracy Theories**
Staff should be aware that children may be exposed to misleading or harmful content online, including misinformation, disinformation, and conspiracy theories. These can distort understanding, foster anxiety, and influence behaviour in ways that pose safeguarding risks.
DSLs should ensure that:

- Pupils are taught critical thinking and media literacy skills through PSHE and digital citizenship curricula.

- Staff are trained to recognise signs that a pupil may be influenced by harmful narratives and how to respond to safeguarding concerns arising.
- Concerns are recorded and escalated appropriately, especially where such content intersects with radicalisation, bullying, or mental health issues.
- Filtering and monitoring systems are reviewed to detect emerging risks related to misinformation and conspiracy content.

## 4. Unacceptable use

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

Unacceptable use of the Trust's ICT facilities includes:

- Using ICT facilities to breach intellectual property rights or copyright.
- Using ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- 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 Trust and/or school, or risks bringing either into disrepute.
- Inappropriate sharing of confidential information about the Trust, school, its pupils, or other members of the school community.
- Connecting any device to the ICT network without approval from authorised personnel.
- Setting up any software, applications, the use of web-based programs 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. Approval needs to be given in the schools' IT Change Management meeting.
- Downloading documents from 365, Network, Google, or approved apps to personal devices.
- Gaining, or attempting to gain, access to restricted areas of the network, or to password-protected information.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the Trust or school's ICT facilities.
- Causing intentional damage to ICT facilities.
- Removing, deleting, or disposing of ICT equipment, systems, programs, or information/data.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access.
- Using inappropriate or offensive language.
- Any form of cyber bullying on the school devices, apps, programs, or network.
- Promoting a private business, unless that business is directly related to the Trust.
- Using websites or mechanisms to bypass the Trust and school's filtering mechanisms.

This is not an exhaustive list. We reserve the right to amend this list at any time. The CEO and school SLTs will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of ICT facilities.

### 4.1 Exceptions from unacceptable use

Where the use of Trust ICT facilities is required for a purpose that would otherwise be considered unacceptable use, exemptions to the policy should be sought from the CEO/HT.

### 4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with school policies: Behaviour Policy, Staff Code of Conduct and Disciplinary and Capability Procedure.

This may include the removal of access or specific functions of ICT provision, as decided by the SLT in the specific school.

Individual school's behaviour policies will cover specific acts of cyber bullying and how they are dealt with.

The Trust's Code of Conduct and Disciplinary and Capability Procedure can be found in MS Teams in the ELT Staff team/General/ELT Policies tab (at the top of the page).

### 4.3 Up to date software

Any device that is issued by the trust or used on trust networks must be running the latest operating system and have all updates including security updates installed.

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

All staff will receive safeguarding and online safety training as part of their induction and regular updates, at least annually, in line with KCSIE guidance.

**All staff will read at least Part One of KCSIE25. Staff who do not work directly with children may read Annex A instead, as determined by the school's leadership.**

### 5.1 Access to Trust ICT facilities and materials

The CEO and school SLT/IT support manage access to the school's ICT facilities. That includes, but is not limited to:

- Computers, laptops, 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.

Staff who inadvertently have access to files, Teams, or channels they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the relevant IT support.

All staff must complete annual cyber security training and follow all training recommendations.

#### 5.1.2 Online Live Lessons

Staff across the trust may be required to deliver remote lessons online. This policy will apply to the use of facilities and materials to conduct these. The running of such sessions is covered by Appendix 6.

#### 5.1.3 Use of phones and email

The school provides each staff member with an email address. This email account should be used for work purposes only. All work-related business should be conducted using this email address.

Staff must not share 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.

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 their IT Support and Trust GDPR manager immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must call with their number being withheld if using their own phone to contact parents or families of the school.

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.

Schools' will not record in-coming and out-going phone conversations.

### 5.2 Personal use

Staff are permitted to 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 CEO or 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 contact time/teaching hours/contracted working hours.
- 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 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.

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

Staff are also permitted to use their personal devices (such as mobile phones or tablets) to access Trust and school cloud infrastructure if this does not constitute 'unacceptable use', as defined in section 4 and has up to date software, as defined in section 4.3.

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 social media considerations (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

The school cannot be held responsible for any loss or damage of personal devices.

#### 5.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is always appropriate. Guidelines for staff on appropriate security settings for social media accounts are contained within appendix 1.

### 5.3 Remote access

The Trust operates a cloud-based ICT solution that is provided by Microsoft. Some schools within the Trust may also use alternative solutions e.g., Google. All documents, interactions, communication, and participation within this solution is deemed to be ICT facilities of the Trust. All files and data within the Microsoft (or alternate) environment are deemed to be materials covered by this policy.

We allow staff to access the other parts of some school's ICT facilities and materials remotely. We offer a remote desktop service which is monitored by IT support. You will need to use your school email and password to access this. Details on how to access this is in the relevant school's staff handbook.

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

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

### 5.4 School social media accounts

These are managed by staff members who have been authorised to manage, or post to, the account. Those without such permission must not access or attempt to access the account.

The Trust has guidelines which support managers of our social media accounts contained within our Communications Policy (external) for what can and cannot be posted, with special care taken regarding picture permission for children in our schools. Those who are authorised to manage the account must ensure they always abide by these guidelines.

### 5.5 Monitoring of school network and use of ICT facilities

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

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

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

Each school monitors ICT use 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.
- Safeguard children and staff.

Staff and pupils will be educated on recognising and reporting harmful sexual behaviour online. Any incidents of online sexual harassment or abuse will be dealt with in line with the school's safeguarding and behaviour policies.

Staff will be supported to understand how to safeguard gender questioning children, including recognising online risks and ensuring appropriate support is in place.

## 6. Pupils

### 6.1 Access to ICT facilities

We will seek to keep children and young people safe by:

- Teaching pupils in all our schools about the opportunities as well as risks and opportunities of online presence
- providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults
- supporting and encouraging all pupils to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person

All trust setting will have appropriate filters and have their networks monitored in accordance with DfE guidance. This will keep children as safe as possible and alert adults to any searches that should be investigated further.

The trust will oversee the procurement of all equipment purchases for each school to ensure consistency in product across all schools. The access granted to students to use these facilities will be at the direction of each school's SLT and the rules they set out relating to use of specific rooms, locations, and equipment during the school day, after hours and off site.

### 6.2 Search and deletion

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

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

### 6.3 Unacceptable use of ICT and the internet outside of school

Schools will sanction pupils, in line with their respective 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 inappropriate.
- Activity which defames or disparages the school, or risks bringing the school into disrepute.

- Sharing confidential information about the school, other pupils, or 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.

## 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 Trust or a 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 HT's discretion. Where parents are granted access in this way, they must abide by this policy.

Parents must not use pupil accounts to communicate with staff. They must use appropriate communication channels as set out by each school. This is likely to be using the parent's own email address to email the relevant member of staff.

We will ensure that personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate. We will ensure that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given.

### 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.
Staff will receive guidance on the safe and ethical use of AI in education, including how to support pupils in using AI tools responsibly.

## 8. Data security

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

### 8.1 Passwords

All users of the Trust 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.

Passwords are required to be updated by all adult users when prompted to by the Trust to provide enhanced security, and in an appropriate time frame for pupils.  Younger pupils will struggle with frequent changes to

their passwords, whereas older pupils will be better able to remember to do this as part of their online security.

Password resets will only be processed when it is verifiable that the owner of the account is requesting this. When a student is not on site and requires a reset, each school will have a specific protocol for doing this to ensure data protection legislation is followed.

### 8.2 Software updates, firewalls, and anti-virus software

All 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 be configured in this way.

### 8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and our Data Protection Policy. Data is always processed fairly and lawfully and information that does need to be kept is done so safely and securely in line with ICO guidance.

### 8.4 Access to facilities and materials

All users of the Trust's ICT facilities will have their access rights to the Trust and specific school systems, files and devices monitored by their line manager. These access rights are controlled by each school's IT support/trust leadership/SLT at the line manager's request.

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 IT Support immediately.

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

### 8.5 Encryption

The Trust and schools ensure that its devices and systems have an appropriate level of encryption. USB memory sticks must not be used. All documents should be accessed and saved within the Microsoft 365 environment using OneDrive and Teams.

## 9. Internet access

Each school's internet connection and Wi-Fi network is secured. The internet is filtered with high level restrictions on what can and cannot be accessed. Filtering and monitoring processes are outlined in our Safeguarding Policy. Should a specific site appear to any staff as being inappropriate, they must notify the Designated Safeguarding Lead (DSL) immediately.

### 9.1 Pupils

Pupil access to Wi-Fi in schools will be managed through acceptable use agreements (Appendix 3 and 4).

### 9.2 Parents and visitors

Parents and visitors to a school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the trust leadership or school SLT/Headteacher.

They will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. a volunteer or as a member of the PTA).

- Visitors need to access the school's Wi-Fi to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan).
- The device is running the latest operating system and has all updates including security updates installed.

## 10. Related policies

This policy should be read alongside the:

- Safeguarding Policy
- Behaviour Policy
- Disciplinary and Capability Procedure
- Code of Conduct/Staff Behaviour
- Data Protection Policy

## Appendix 1: Social media considerations for staff

**Don't accept friend requests from pupils on social media**

### 10 considerations for school staff on social media platforms

1. Change your display name for personal accounts– 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/employer.
6. Don't use social media sites during school hours.
7. Don't make comments about your job, colleagues, school, or 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) can find you using this information.
10. Do not activate desktop or browser notifications on a work device as this may interfere with the delivery of a lesson.
11. Consider uninstalling social media apps from your phone, The app recognises wi-fi connections and makes friend suggestions based on who else uses the same wi-fi 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.
- If you require any assistance with your adjusting your privacy settings on social media, please contact the ICT Helpdesk – helpdesk@esherhigh.surrey.sch.uk.
- 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 be able to see posts you've **'liked'**, even if your profile settings are private, as 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 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.

### 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 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

| Acceptable use of the internet: agreement for parents and carers | |
|---|---|
| **Name of parent/carer:**<br><br>**Name of child:** | |
| Online channels are an important way for parents/carers to communicate with, or about, our school.<br>The school uses the following channels:<br>• Email/text for parents (for school announcements and information)<br>• School communication apps (E.g.: Edulink One/Scopay/School comms) | |
| When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:<br>• Be respectful towards members of staff, and the school, at all times.<br>• Be respectful of other parents/carers and children.<br>• 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.<br>I will not:<br>• Use my child's school account (including email and Teams) to attempt to communicate with the school, I will use the approved communication avenues to contact staff (e.g. email, phone call, EduLink One).<br>• Use private groups, the school's social media accounts, community social media accounts, WhatsApp or personal social media to complain about or criticise members of staff or the school. This is not constructive, and the school can't improve or address issues if they aren't raised in an appropriate way.<br>• Use private groups, social media accounts, community social media accounts, WhatsApp, 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.<br>• Upload or share photos or videos on social media or via text message/WhatsApp of any child other than my own unless I have the permission of other children's parents/carers. | |
| **Signed**: | **Date:** |

## Appendix 3: Acceptable use agreement for older pupils

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

**Name of pupil:**

**When using the school's ICT facilities and accessing the internet in school, I will:**

- Use them for educational purpose.
- Use them with a teacher being present, or with a teacher's permission.
- Only access any appropriate websites.
- Only access social networking sites if my teacher has expressly allowed this as part of a learning activity.
- Use appropriate language when communicating online, including in emails.

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

- Use artificial intelligence without oversight of a teacher.
- Submit work that I have not produced myself.
- Use chat rooms that are not authorised by the school.
- Open any attachments, or follow any links, without first checking with a teacher.
- Use any image of another student or member of the public as my profile picture.
- Share my password with others or log in to the school's network using someone else's details.
- Bully others.
- Use them to break school rules.

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

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

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

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

| **Signed (pupil):** | **Date:** |
|---|---|

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

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

## Appendix 4: Acceptable use agreement for younger pupils

| **Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers** | |
|---|---|
| **Name of pupil:** | |
| **When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will:**<br>• Use them for learning.<br>• Use them with a teacher being present, or with a teacher's permission.<br>• Only access appropriate websites.<br>**When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not:**<br>• Use artificial intelligence without oversight of a teacher.<br>• Submit work that I have not produced myself.<br>• Open any attachments in emails, or click any links in emails, without checking with a teacher first.<br>• Use unkind or rude language when talking to people online or in emails.<br>• Share my password with others or log in using someone else's name or password.<br>• Bully others.<br>• Use them to break school rules.<br><br>I understand that the school/Trust will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.<br>I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.<br>I will always be responsible when I use the school's ICT systems and internet.<br>I understand that there will be consequences in line with our behaviour policy if I do certain unacceptable things online, even if I'm not in school when I do them. | |
| **Signed (pupil):** | **Date:** |
| **Parent/carer agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. | |
| **Signed (parent/carer):** | **Date:** |

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

| **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:<br>• 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).<br>• Use them in any way which could harm the school's reputation.<br>• Use any improper language when communicating.<br>• Install any unauthorised software or connect unauthorised hardware or devices to the school's network.<br>• Share my password with others or log in to the school's network using someone else's details.<br>• Share confidential information about the school, its pupils or staff, or other members of the community.<br>• Access, modify or share data I'm not authorised to access, modify or share.<br>• Promote private businesses unless that business is directly related to the school.<br>• Store images of students or student personal data on personal devices. | |
| I understand that the School/Trust will monitor the websites I visit and my use of the school's ICT facilities and systems.<br>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.<br>I confirm that any device used on trust networks is running the latest operating system and has all updates including security updates installed.<br>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, and will also do so if I encounter any such material.<br>I will always use the school's ICT systems and internet responsibly, abiding by the ICT and Acceptable Use Policy, Cyber Security training and guidance, and ensure that pupils in my care do so too. | |
| **Signed (staff member/governor/volunteer/visitor):** | **Date:** |

## Appendix 6: Online Live Lesson Acceptable Use Policy (AUP)

**Leadership Oversight and Approval**

Remote learning will only take place using Microsoft Teams or Google Classroom. These environments have been assessed and approved by the Headteacher and the Senior Leadership Team (SLT) of each school.

Staff will only use school accounts with learners and parents/carers. Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.

Staff will use work provided equipment where possible. e.g. a school laptop, tablet, or other mobile device.

All remote lessons will be formally timetabled; and scheduled in the specific class channel. Another colleague can be invited to support in the lessons. School leaders can be invited and should be able to drop in at any time.

Live streamed remote learning sessions will only be held during the agreed and published times by the SLT.

**Data Protection and Security**

1. Any personal data used by staff and captured by Microsoft Teams/Google Classroom when delivering remote learning will be processed and stored with appropriate consent and in accordance with the ELT data protection policy.
2. All remote learning and any other online communication will take place in line with current ELT confidentiality expectations as outlined in ELT Code of Conduct.
3. All participants will be made aware that Microsoft Teams/Google Classroom records activity and that remote lessons are being recorded and stored on the ELT Microsoft platform or Google Drive.
4. Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by SLT and in line with our data protection requirements.
5. Only members of ELT community will be given access to Microsoft Teams or Google Drive.
6. Access to Microsoft Teams/Google drive will be managed in line with current IT security expectations as outlined in the ELT ICT policy.

**Session Management**

1. Staff will schedule and ensure the correct class, time, and date of any sessions held are done using the correct method in Teams for their class.
2. Appropriate privacy and safety settings will be used to manage access and interactions.
3. When live streaming with learners:
    - Contact will be made via learners' school provided email accounts and subsequent Microsoft Teams logins.
    - Staff will ask the student to disable their video/mute their microphone at their discretion.
    - Staff can remove the student from the lesson if they do not follow instructions.
4. It will be at the lead teacher's discretion if they would like students to use their camera later in the lesson to see students. This will be done whilst reminding students to be appropriately dressed and to use a blurred or picture background. Lessons will be recorded to safeguard all involved.
5. Live 1 to 1 sessions can take place with approval from a member of the SLT.
    - In this scenario a parent/carer is to be present in the room and a 2nd member of staff on the call. If this is not possible, the session must still be recorded.
6. Access links are not to be made public or shared by participants.
    - Learners and/or parents/carers must not forward or share access links.

- If learners/parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first who will seek permission from a member of the SLT.

7. Learners are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.

**Behaviour Expectations**

1. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
2. All participants are expected to behave in line with existing school policies and expectations.
3. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
4. When live streaming, participants are required to:
    - Ensure student cameras are to be switched off (at the teacher's/leader's discretion).
    - Wear appropriate dress in case of a camera being accidentally turned on.
    - Check that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.

*All Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.*

**Policy Breaches and Reporting Concerns**

Participants are encouraged to report concerns during remote sessions:

1. If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated and concerns will be recorded on Arbor/CPOMS, reported to the line manager/HOD and DSL if a safeguarding concern.
2. Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying, and behaviour.
3. Sanctions for deliberate misuse may include, restricting/removing use, contacting police if a criminal offence has been committed.

## Appendix 7: ELT Online Live Lessons Acceptable Use Agreement

As we use Cloud based environments to run online lessons, it is important that pupils are aware of the way they need to conduct themselves in this way of working. Below are the main points that need to be followed to ensure that learning is productive in this new way of working.

**All lessons will be recorded for safeguarding purposes. By entering the lessons, you agree to this.**

**What we ask of you:**

- Be ready to start your lessons on time.
- Be polite to our teachers and friendly to other learners.
- If you have something you would like to contribute or ask, type in the chat box, your teacher will invite you to unmute if needed. The chat function is for learning based comments or questions, not a social area.
- Respect other people's opinions and ideas.
- Always try your best in all that you do.

**Display safe online behaviour:**

- Please switch your camera off before entering the lesson.
- Be appropriately dressed. Just in case your camera turns on accidently.
- Do not give your personal contact details to anyone else in your online class.
- Remember everything you do on the internet can be seen by someone else.
- Ignore inappropriate online behaviour by others, our teachers will deal with this.
- Be responsible for everything you do and say online.

**Our teachers will not tolerate:**

- Bullying includes discriminatory, offensive, aggressive, or unpleasant language or threats. All are unacceptable – this may result in removal from our classroom.
- Abuse of your microphone - this will result in your microphone being muted.
- Abuse of the chat box – this may result in you being removed.
- Students should not record the lesson on your device or any other device.

## Appendix 8 ELT Online Safety educational aims

In **Key Stage 1**, pupils will be taught to:

- 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.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully, and responsibly, recognising acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content, and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- How to respond safely and appropriately to adults they may encounter whom they do not know.

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly, and securely, including protecting their online identity and privacy.
- Recognise inappropriate content, contact, and conduct, and know how to report concerns.

Pupils in **Key Stage 4** will be taught:

- How changes in technology affect safety, including ways to protect their online privacy and identity.
- How to report a range of concerns.

By the **end of secondary school**, they will know:

- Their rights, responsibilities, and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report material or manage issues online.
- The impact of viewing harmful content including sexually explicit material (e.g. pornography) which may present a distorted picture of sexual behaviour and can therefore damage the way people see themselves and negatively affect how they behave towards sexual partners.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail.
- How information and data is generated, collected, shared, and used online.
- How to identify harmful behaviours online (including bullying, abuse, or harassment) and how to report, or find support, if they have been affected by those behaviours.
- How to identify misinformation and disinformation, understanding sources, and evaluating credibility.