



THE CHURCH
OF ENGLAND

Lady Boswell's C.E. (Aided)
Primary School

*Learning Together,
Christ at the Centre,
Learning for Life*

ICT and Internet Acceptable Use
Policy (AUP)

(For Staff, Governors, Volunteers,
Pupils & Visitors)

Date of Policy: January 2025

Approved: January 2025

Date of Next Review: January 2028

Policy authorised by:

Sharon Saunders and Hannah Pullen

Co-Headteachers

Signature:

Author of Policy: Hannah Browning

We value every member of our community as a unique child of God and seek to demonstrate His love through our words and actions. We enable every child to achieve their full potential so that they leave us with their heads inspired and their hearts enriched.

As a result, our children will:

Develop a positive sense of self and well-being; confident to make the right choices and keep themselves safe in an ever-changing society

Strive for academic excellence, developing a thirst for knowledge and a love of learning

Become effective communicators, collaborators and leaders

Be resilient, resourceful and courageous

Be curious, creative individuals and confident problem solvers

Grow in spiritual awareness and develop a strong moral compass and a deepening understanding of the Christian faith in a multi-faith British society

Become responsible and tolerant global citizens who value diversity, forgive readily, and have concern for the needs of each other, the school, the wider community, and the planet.

Contents

1. Introduction and aims	3
2. Relevant legislation and guidance	4
3. Definitions	4
4. Unacceptable use	5
5. Staff (including governors, volunteers and contractors)	6
6. Pupils	8
7. Parents/carers	10
8. <u>Data security</u>	11
9. <u>Protection from cyber attacks</u>	12
10. Internet access	133
11. Monitoring and review.....	14
12. Related policies	14

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. 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, volunteers 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 (Positive Learning and Wellbeing Policy), staff code of conduct, governor code of conduct and volunteer 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 UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)
- [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](#)
- [Education and Inspections Act 2006](#)
- [Keeping Children Safe in Education 2023](#)
- [Searching, screening and confiscation: advice for schools 2022](#)
- [National Cyber Security Centre \(NCSC\): Cyber Security for Schools](#)
- [Education and Training \(Welfare of Children\) Act 2021](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- [Meeting digital and technology standards in schools and colleges](#)

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 (including photocopiers), software, websites, web applications or services, WIFI, 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 agreed by an authorised user
- **“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
- 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 (School Business Manager, Member of SLT, Network Manager)
- 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 Co-Headteachers 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 Co-Headteacher's discretion.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on behaviour/ staff code of conduct and mobile phone policies which can be viewed via the school network.

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

5.1 Access to school ICT facilities and materials

The school's Network Manager 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 network manager, School Business Manager or a member of the SLT.

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. Staff should enable multi-factor authentication on their email account(s).

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 highly 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 that contains the personal information of another person, they must inform the Co-Headteachers, School Business Manager and Network Manager immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Only in exceptional circumstances should staff telephone parents from their personal devices. Where is unavoidable, staff should take steps to withhold their number.

School phones must not be used for personal matters, unless in exceptional circumstances, authorised by a member of the SLT.

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

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Co-Headteachers/ Network manager 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/non-break time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

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

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

Staff are permitted to use their personal devices (such as mobile phones or tablets) in line with the school's mobile phone policy.

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

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

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

5.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely. They should dial in using a virtual private network (VPN) which is managed by **MEDWAY GRID FOR LEARNING** or via Google Classroom/ Google Drive where some school documents are stored.

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 Network Manager 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 which can be viewed on the school website.

5.4 Monitoring and filtering of school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls

- User activity/access logs
- Any other electronic communications

Only authorised ICT/ Safeguarding staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The effectiveness of any filtering and monitoring will be regularly reviewed. Where appropriate, authorised personnel may raise concerns about monitored activity with the school's designated safeguarding lead (DSL), as appropriate.

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

Our governing body is responsible for making sure that:

- The school meets the DfE's [filtering and monitoring standards](#)
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
 - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and Network manager, as appropriate.

6. Pupils

6.1 Access to ICT facilities

A range of ICT facilities are available to pupils:

- Computers, iPads and equipment in the school's ICT suite are available to pupils only under the supervision of staff. Year 6 pupils may use the computers in the ICT suite independently for educational purposes only where permission from the Year 6 teachers has been sought.
- 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 the school's virtual learning environment, which they can access from any device as well as a login to their designated class area on Google Classroom.

6.2 Search and deletion

Under the Education Act 2011, the Co-headteacher, and any member of staff authorised to do so by the Co-headteacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out and/or
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Further information about the school's protocols for searching, screening and confiscation can be found in the school's safeguarding policy.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Co-Headteacher / designated safeguarding lead / SLT
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation (if the pupil refuses to co-operate, we will proceed according to our behaviour policy)
- The authorised staff member should:
- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item. A list of banned items is available
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL / Co-Headteacher / other member of the Senior Leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image

- Not copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy and safeguarding policy.

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

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

Where appropriate, this will be done in conjunction with parents.

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 Co-Headteacher's discretion.

Where parents/carers 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/carers to sign the agreement in appendix 2.

7.3 Communicating with parents/carers about pupil activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

8. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on [digital and technology standards in schools and colleges](#), including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

8.1 Passwords

All adult 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 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.

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 which can be found on the school website.

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 network manager CANTIUM BUSINESS SOLUTIONS.

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 Co- Headteacher/ Network Manager 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 shut down completely at the end of each working day.

8.5 Encryption

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

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

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Co-Headteacher/ Network Manager.

9. Protection from cyber attacks

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

The school will:

- Work with governors, **Medway Grid for Learning** and Cantium Business Solutions to make sure cyber security is given the time and resources it needs to make the school secure
- Provide **regular** training for staff and new staff within the induction pack 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 annually, 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 daily and store these backups with Cantium Business Solutions
 - Delegate specific responsibility for maintaining the security of our management information system (MIS) to Cantium Business Solutions
 - 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'

10. Internet access

The school's wireless internet connection is secure.

The School has 2 methods of wifi access – school and guest.

All PCs on the network will use the school wifi.

Any visitors to the school will use the guest wifi, **which is protected by a token system.**

The School's filtering system is Netsweeper, which meets all the required standards for School Education filtering.

Any inappropriate sites found will be reported to our ICT support team.

Wifi for the school, including filtering is provided via **Medway Grid for Learning**

10.1 Pupils

- Wi-Fi is available throughout the school site. Pupils can access the internet under adult supervision via computers and iPads.
- Filtering and monitoring is provided by **Medway Grid for Learning**
- Pupils must either be logged in to a school computer or use an iPad allocated to them to access the internet

10.2 Parents and visitors

Parents/carers and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the Co- Headteacher.

The Co-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)

Once they have been authorised, parents/carers and visitors will be given a coded voucher to access the guest wifi, and will be asked to agree to the terms of acceptable use.

11. Monitoring and review

The Co-Headteacher and Network Manager. 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 body is responsible for approving this policy.

12. Related policies

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

- Child Protection / Safeguarding Policy (Encompassing On-Line Safety)
- Behaviour Policy and Principles
- Staff Discipline & Conduct
- GDPR & Data Protection
- Remote Learning Policy
- Mobile phone Policy

Also, the school's Acceptable Use Agreements for:

- Parent and Carers
- Staff and Volunteers
- Community Users
- EYFS and KS1
- KS2
- Use of AI
- Responding to incidents of misuse flowcharts

These are all available from the School Office.

Signed:	Date:
Print Name:	

