

CHANCERY EDUCATION TRUST

DATA SECURITY, E-SAFETY POLICY & ACCEPTABLE USE AGREEMENT

SEPTEMBER 2025

Next Review Date: September 2026

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Chancery Education Trust – Data Security, E-Safety Policy & Acceptable Use Agreement – September 2025

Executive Summary for CET Data Security, E-Safety Policy & Acceptable Use Agreement September 2025:

Purpose and Scope

- Aligns with UK GDPR and the Data Protection Act 2018 to safeguard personal and sensitive data.
- Covers all written, spoken, and electronic information, whether on IT systems, paper, mobile devices, or orally shared
- Applies to all staff, contractors, volunteers, governors, pupils, and parents.
- Breaches may result in disciplinary action up to dismissal

Roles and Responsibilities

- Headteacher & SLT: Ensure e-safety, oversee training, and create monitoring systems.
- E-Safety Coordinator: Daily responsibility, incident logging, training, escalation of serious issues
- Network/IT Staff: Maintain secure infrastructure, enforce password policies, monitor network use, and perform regular backups.
- Teaching & Support Staff: Embed e-safety in teaching, model safe use, and report misuse
- Designated Safeguarding Leads (DSL/DDSL): Handle risks such as grooming, cyberbullying, sexting.
- Pupils: Learn safe digital use, avoid plagiarism, understand risks, report abuse, respect age limits on social media
- Parents/Carers: Support safe use at home, follow image and internet use guidelines.

Data Security Measures

- Physical Security: Lock documents, secure classrooms, restricted visitor access, CCTV monitoring
- IT Security:
 - Passwords must be strong, private, and regularly updated.
 - Devices must lock after inactivity; unauthorised access is forbidden.
 - All data backed up securely and stored off-site
- Access & Storage:
 - Only authorised staff access sensitive data.
 - Portable devices and drives must be encrypted.
 - No personal storage of school data without approval

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

- Communications:
 - Emails, post, and digital transfers must be encrypted/secure.
 - Addresses and recipients must always be double-checked.

E-Safety in Practice

- Curriculum: Pupils taught about online dangers (inappropriate content, online contact, commercial risks).
- Staff Use:
 - Official systems only for digital communication.
 - Cloud storage allowed only if password protected.
- Incident Handling:
 - All breaches must be reported immediately to senior staff.
 - Full documentation required (linked to Data Breach Policy).
 - *Flowchart on page 17* outlines reporting of incidents from unsuitable material to illegal content.
- Monitoring: Email, internet, and device use is logged and may be monitored at all times

Social Media & Images

- Pupils under 13 cannot have social media accounts.
- Staff must not use personal accounts for school communication.
- School-run social media pages are strictly controlled; inappropriate comments are removed.
- Parents may take photos at school events but must not post them online.
- Images of pupils are only used with parental consent, stored securely, and managed via school equipment

Acceptable Use Agreements

- Staff (Appendix 2): Must sign agreement covering professional IT use, password security, safe use of devices, social media conduct, and safeguarding obligations
- Pupils (Appendix 3):
 - Junior pupils pledge safe internet use (no sharing personal info, reporting unsuitable content, no chatrooms).
 - Infant pupils (illustrated agreement on *page 26*) commit to using the internet only with adult supervision, keeping passwords private, and being polite online.

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

- Sanctions (page 22): Breaches (e.g., illegal material, misuse of data, inappropriate emails, or bypassing filters) may lead to disciplinary action, HR involvement, police referral, or dismissal

Governance

- Reviewed annually, or sooner if legislation or threats change.
- Approved by CET Board and Governing Boards, with the next review scheduled for September 2026

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Chancery Education Trust – Data Security, E-Safety Policy & Acceptable Use Agreement – September 2025



CHANCERY EDUCATION TRUST

DATA SECURITY, E-SAFETY POLICY & ACCEPTABLE USE AGREEMENT

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

Chancery Education Trust embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communication technologies.

The Trust seeks to prevent any safeguarding issues including cyber-bullying, through the rigorous application of this policy. The E-Safety of staff and pupils is of utmost importance and the Trust seeks to avoid inappropriate or misguided use, which may expose both adults and young people to unacceptable risks and dangers, including cyber-bullying.

To that end, the Trust aims to provide a safe and secure environment, which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

This document sets out the measures taken by the Academy School to achieve this, including to:

- protect against potential breaches of confidentiality;
- ensure that all information assets and IT facilities are protected against damage, loss or misuse;
- support our Data Protection and SAR Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and
- Increase awareness and understanding at the Academy School of the requirements of information security and the responsibility to staff to protect the confidentiality and integrity of the information that they themselves handle.

The use by staff and monitoring by the Academy School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner.

Scope

The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the Trust/Academy School, in whatever media. This includes information held on computer systems, paper records, hand-held devices, and information transmitted orally.

On joining the Trust, the individual Academy School will provide new joiners/voluntary staff or those undertaking work experience a copy of the Data Security, E-Safety policy and Acceptable Use Agreement to read and sign to demonstrate that they have understood and will adhere to the procedures set out in the E-Safety policy and Acceptable Use

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Agreement. Signed copies of the Acceptable Use Agreement will be retained in their personnel file. (See Appendix 2)

This policy applies to all members of staff, including temporary workers, other contractors, volunteers, interns, governors and any and all third parties authorised to use the IT systems.

All members of staff are required to familiarise themselves with its content and to comply with the provisions contained within it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the Trust and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

The Data Security, E-Safety policy and Acceptable Use Agreement will be reviewed on an annual basis and if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The policy is on the Academy School website.

This policy, supported by the Academy School's acceptable use agreement, is to protect the interests and safety of the whole Academy School community.

Each Academy School has a named E-Safety co-ordinator:

The E-Safety co-ordinator for Darrick Wood Infant & Nursery School is Mrs Lydia Crawford

The E-Safety co-ordinator for John Wood School & Nursery is Miss Serena Annor

The E-Safety co-ordinator for Pickhurst Academy is Mrs Holly Hewitt

The E-Safety co-ordinator's for Oaklands Primary Academy are Miss Sue Brotherhood and Miss Jade Lurkins

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Chancery Education Trust – Data Security, E-Safety Policy & Acceptable Use Agreement – September 2025



Roles and Responsibilities

Role	Key Responsibilities
Headteacher/Principal and Senior Leadership Team (SLT)	- The Headteacher/Principal has a duty of care for ensuring the safety (including E-Safety) of members of the Academy School community - The Headteacher/Principal and (at least) another member of the SLT should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff - The Headteacher/Principal and Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues, as relevant - The Headteacher/Principal will ensure that there is a system in place to allow for monitoring and support of those in the Academy School who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles - The Headteacher/Principal will form an E-Safety group including representatives of SLT, teaching staff, students and parents to ensure that the E-Safety policy is applied consistently and is relevant, taking into account developments and new technology
The E-Safety Coordinator	- Takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the Trusts E-Safety policies / documents - Ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place - Provides training and advice for staff and parents - Logs and monitors E-Safety incidents. Serious incidents must be escalated immediately to the Headteacher/Principal/DSL - Organises E-Safety week and safer internet day

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

The Network Manager / Technical staff	• Ensure that the Academy School's technical infrastructure is secure and is not open to misuse or malicious attack • Ensure that the Academy School meets required E-Safety technical requirements and any Local Authority/other relevant body/ E-Safety Policy guidance that may apply • Ensure that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed • Keep up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant • Monitor the use of the network/internet / Virtual Learning Environment/remote access/email is checked regularly, in order that any misuse or attempted misuse can be reported to the Headteacher/Principal/E-Safety co-ordinator
Teaching, and Support Staff, including MDS	• They have an up to date awareness of E-Safety matters and of the current Academy School E-Safety policy and practices • They have read, understood and signed the Staff Acceptable Use Agreement • They report any suspected misuse or problem to the Headteacher/Principal/E-Safety co-ordinator for investigation/action/ sanction • All digital communications with students/pupils/parents/carers are on a professional level and only carried out using official Trust systems • E-Safety issues are embedded in all aspects of the curriculum and other activities • Students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other Academy School activities (where allowed) and implement current policies with regard to these devices • In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

	Exit strategy At the end of the period of employment/ volunteering all equipment and devices loaned by the Academy School must be returned, this will include leaving PINs, IDs and passwords to allow devices to be reset, or to meet with line manager and technician on the last day to log in and allow a factory reset.
Designated Safeguarding Lead (DSL) Deputy Designated Safeguarding Lead (DDSL)	The designated safeguarding lead (DSL) has responsibility for “understanding the filtering and monitoring systems and processes in place” as part of their remit. They will be trained in E-Safety issues and be aware of the potential for serious child protection/ safeguarding issues to arise from: - Sharing of personal data - Access to illegal/inappropriate materials - Inappropriate on-line contact with adults/strangers - Potential or actual incidents of grooming - Cyber-bullying - Sexting
Pupils	At age appropriate levels - Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations - Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so - Know and understand policies on the taking/use of images and on cyber-bullying - Should understand the importance of adopting good E-Safety practice when using digital technologies out of school - Be made aware that children under the age of 13 are not legally allowed to use social media channels such as Facebook, Instagram, Twitter etc.

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Parents / Carers	Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/ mobile devices in an appropriate way. The Academy School will take every opportunity to help parents understand these issues through parents' information meetings, newsletters, letters, website and information about national/local E-Safety campaigns/literature. Parents and carers will be encouraged to support the Academy School in promoting good E-Safety practice and to follow guidelines on the appropriate use of: • Digital and video images taken at Academy School events • Access to parents' sections of the website • Supporting children in the use of the VLE at home Parents must be mindful that children under the age of 13 are not legally allowed to use social media channels such as Facebook, Instagram, X etc.
-------------------------	---

General Principles

All data stored on our IT Systems are to be classified appropriately (including, but not limited to personal data, sensitive personal data and confidential information. Further details on the categories of data can be found in the Academy School's Data Protection Policy and Record of Processing Activities). All data so classified must be handled appropriately in accordance with its classification.

Staff should discuss with the Headteacher/Principal the appropriate security arrangements for the type of information they access in the course of their work.

All data stored within our IT Systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

All IT Systems are to be installed, maintained, serviced, repaired and upgraded by Classroom 365 or by such third party/parties as the Trust may authorise.

The responsibility for the security and integrity of all IT Systems and the data stored thereon (including but not limited to the security, integrity and confidentiality of that data) lies with Classroom 365 unless expressly stated otherwise.

All staff have an obligation to report actual and potential data protection compliance failures to CEO/Headteacher/Principal who shall investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer (full details of the officer can be found in our Data Protection Policy).

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Physical Security and Procedures

Paper records and documents containing personal information, sensitive personal information and confidential information shall be positioned in a way to avoid them being viewed by people passing by as far as possible, e.g. through windows. At the end of the working day or when you leave your desk unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.

Available locked cabinets and other storage systems with locks shall be used to store paper records when not in use. If you do not feel you have appropriate and/or sufficient storage available to you, you must inform the Headteacher/Principal as soon as possible.

Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of school.

The physical security of buildings and storage systems shall be reviewed on a regular basis. If you find the security to be insufficient, you must inform Headteacher/Principal as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

The following measures are taken by the Academy School to ensure physical security of the building/s and storage systems:

- The Academy School carry out regular checks of the buildings and storage systems to ensure they are maintained to a high standard
- The Academy School has an intercom system to minimise the risk of unauthorised people from entering the school premises
- The Academy School close the school gates during certain hours to prevent unauthorised access to the building. An alarm system is set nightly
- CCTV Cameras are in use at the Academy School and monitored by the Caretaker
- Visitors should be required to sign in at the reception, accompanied at all times by a member of staff and never be left alone in areas where they could have access to confidential information

Computers and IT

The Headteacher/Principal/IT shall be responsible for the following:

- a) ensuring that all IT Systems are assessed and deemed suitable for compliance with the Academy School's security requirements;
- b) ensuring that IT Security standards within the Academy School are effectively implemented and regularly reviewed, working in consultation with the Academy School's management and reporting the outcome of such reviews to the Academy School's management;
- c) ensuring that all members of staff are kept aware of this policy and of all related legislation, regulations and other relevant rules whether now or in the future in force, including but not limited to the UK GDPR and the Computer Misuse Act 1990.

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and 11 expects all staff and volunteers to share this commitment.

Furthermore, the Headteacher/Principal/IT shall be responsible for the following:

- a) assisting all members of staff in understanding and complying with this policy;
- b) providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems;
- c) ensuring that all members of staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities and any special security requirements;
- d) receiving and handling all reports relating to IT Security matters and taking appropriate action in response [including, in the event that any reports relate to personal data, informing the Data Protection Officer];
- e) taking proactive action, where possible, to establish and implement IT security procedures and to raise awareness among members of staff;
- f) monitoring all IT security within the Academy School and taking all necessary action to implement this policy and any changes made to this policy in the future; and
- g) ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

Responsibilities – Members of Staff

All members of staff must comply with all relevant parts of this policy at all times when using the IT Systems.

Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.

You must immediately inform CEO/Headteacher/Principal of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the Data Breach Policy.

Any other technical problems (including but not limited to, hardware failures and software errors) which may occur on the IT Systems shall be reported to the IT immediately.

You are not permitted to install any software of your own without the approval of the IT. Any software belonging to you must be approved by the IT and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.

Prior to installation of any software onto the IT Systems, you must obtain written permission by Headteacher/Principal/IT. This permission must clearly state which software you may install and onto which computer(s) or device(s) it may be installed.

Prior to any usage of physical media (e.g., USB memory sticks or disks of any kind) for transferring files, you must make sure to have the physical media virus scanned. Approval from Headteacher/Principal must be obtained prior to transferring of files using cloud storage systems.

If you detect any virus this must be reported immediately to IT (this rule shall apply even where the anti-virus software automatically fixes the problem).

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and 12 expects all staff and volunteers to share this commitment.

Access Security

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

The Academy School has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the Academy School's network. The Academy School also teach individuals about e-safety to ensure everyone is aware of how to protect the Academy School's network and themselves.

All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by the IT Department. Biometric log-in methods can only be used if approved by the IT Department.

All passwords must, where the software, computer, or device allows:

Passwords should be at least 6-8 characters containing a mixture of letters (both upper and lower case), numbers (digits 0-9) and symbols (eg. !"£\$%^&*).

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Group who will liaise with IT as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If you forget your password you should notify IT to have your access to the IT Systems restored. You must set up a new password immediately upon the restoration of access to the IT Systems.

You should not write down passwords if it is possible to remember them. If necessary, you may write down passwords provided that you store them securely (e.g., in a locked drawer or in a secure password database). Passwords should never be left on display for others to see.

Computers and other electronical devices with displays and user input devices (e.g., mouse, keyboard, touchscreen etc.) shall be protected with a screen lock that will activate after a period of inactivity. You may not change this time period or disable the lock.

All mobile devices provided by the Academy School shall be set to lock, sleep or similar after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar. You may not alter this time period.

Staff should be aware that if they fail to log off and leave their terminals unattended, they may be held responsible for another user's activities on their terminal in breach of this

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and 13 expects all staff and volunteers to share this commitment.

policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

E-Safety in the Curriculum

The Academy School provides opportunities within a range of curriculum areas to teach about E-Safety.

Educating pupils on the dangers of technologies that maybe encountered outside the Academy School is done informally when opportunities arise and as part of the E-Safety curriculum.

The teaching of E-Safety focuses on helping children to recognise inappropriate content, conduct, contact and commercialism and helps them learn how to respond or react appropriately.

Pupils are aware of the impact of online bullying and sexting and know how to seek help if they are affected by any of these issues.

Security, Data and Confidentiality

All staff read and sign an Acceptable Use Agreement to demonstrate that they have understood the Academy School's E-Safety Policy.

Staff may, in some circumstances, use cloud based storage, which is password protected to store and access information conveniently

Staff should be aware of their responsibilities when accessing sensitive Academy School data:

- Academy School data will only be accessed by staff, using their own username and password
- Passwords are kept secure and are not shared with another member of staff
- Workstations are locked when left unattended
- Academy School data will not be duplicated onto personally owned equipment
- Portable devices are encrypted and data can only be accessed using a secure log in

Data security

Personal data sent over the school network will be encrypted or otherwise secured.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the CEO who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins. Where consent is given all files and data should always be virus checked before they are downloaded onto the School's systems.

You may connect your own devices (including, but not limited to, laptops, tablets, and smartphones) to the Academy School's Wi-Fi provided that you follow the CEO's requirements and instructions governing this use. All usage of your own device(s) whilst

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and 14 expects all staff and volunteers to share this commitment.

connected to the Academy School's network or any other part of the IT Systems is subject to all relevant Academy School Policies (including, but not limited to, this policy). The CEO may at any time request the immediate disconnection of any such devices without notice.

Electronic storage of data

All portable data, and in particular personal data, should be stored on encrypted drives using methods recommended by the CEO.

All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.

You should not store any personal data on any mobile device, whether such device belongs to the Academy School or otherwise without prior written approval of the CEO. You should delete data copied onto any of these devices as soon as possible and make sure it is stored on the Academy School's computer network in order for it to be backed up.

Staff are responsible for ensuring they have rights for the storage of any file in their area for example, copyright music files.

All electronic data must be securely backed up by the end of the each working day and is done by the responsible person.

Homeworking

Please refer to the Home Working Policy.

Communications, Transfers, Internet and Email Use

There are restrictions on international transfers of personal data and transfers to international organisations. Staff may only transfer personal data outside the UK or to any international organisation, with the prior written authorisation of the DPO. You should refer to the Schools Data Protection policy for further information on international transfers.

The Academy School work to ensure the systems do protect pupils and staff and are reviewed and improved regularly.

If staff or pupils discover unsuitable sites or any material which would be unsuitable, this should be reported to the Headteacher/Principal.

Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee and the Academy School cannot accept liability for the material accessed or its consequence.

All personal information and in particular sensitive personal information and confidential information should be encrypted before being sent by email or sent by tracked DX (document exchange) or recorded delivery.

Postal, DX and email addresses and numbers should be checked and verified before you send information to them. In particular you should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and 15 expects all staff and volunteers to share this commitment.

You should be careful about maintaining confidentiality when speaking in public places.

You should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for the Academy School.

Personal or confidential information should not be removed from the Academy School without prior permission from Headteacher/Principal except where the removal is temporary and necessary. When such permission is given, you must take all reasonable steps to ensure that the integrity of the information and the confidentiality are maintained. You must ensure that the information is:

- a) not transported in see-through or other un-secured bags or cases;
- b) not read in public places (eg. waiting rooms, cafes, trains, etc.); and
- c) not left unattended or in any place where it is at risk (eg. in car boots, cafes, etc.)

Reporting Security Breaches

All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the CEO/Headteacher/Principal. All members of staff have an obligation to report actual or potential data protection compliance failures.

When receiving a question or notification of a breach, the CEO/Headteacher/Principal shall immediately assess the issue, including but not limited to, the level of risk associated with the issue and shall take all steps necessary to respond to the issue.

Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the CEO/Headteacher/Principal. Any attempt to resolve an IT security breach by a member of staff must be under the instruction of and with the express permission of the CEO/Headteacher/Principal.

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to CEO/Headteacher/Principal.

All IT security breaches shall be fully documented.

Full details on how to notify of data breaches are set out in the Data Breach Policy.

Infrastructure/ filtering and monitoring

The Academy School will be responsible for ensuring that their infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their E-Safety responsibilities:

- The Technical systems will be managed in ways that ensure that the Academy School meets recommended technical requirements
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the Academy School systems and

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and 16 expects all staff and volunteers to share this commitment.

data. These are tested regularly. The Academy School infrastructure and individual workstations are protected by up to date virus software

- Personal data cannot be sent over the internet or taken off site
- Staff and pupils are aware that Academy School based email and Internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the incident should be reported immediately to the teacher and then passed on to the Headteacher/Principal/E-Safety coordinator
- If there are any issues related to viruses or anti-virus software, the E-Safety co-ordinator should be informed

Mobile Devices and Smart Technology

Please refer to the Mobile Devices and Smart Technology Policy.

Managing email

The use of email within the Academy School is an essential means of communication for staff.

Where pupils have been set up with individual email accounts, monitoring checks for inappropriate content and if detected forwarded to the Headteacher/Principal and the E-Safety Coordinator. All emails are permanently stored even if deleted by individual users.

Staff must use the Academy School's approved email system for any Academy School related business.

Everyone in the Academy School community understands that the e-mail system is monitored and should not be considered private communication

- Staff must inform the Headteacher/Principal/E-Safety co-ordinator if they receive an offensive or inappropriate e-mail

Social Networking

The Academy School does not permit the pupils to access their private accounts on social or gaming networks at any time during the Academy School Day.

Pupils under the age of 13 should not be allowed access to, or be encouraged to create their own personal social media accounts. Children under the age of 13 are not legally allowed to use social media channels such as Facebook, Instagram, X etc. However, pupils may be encouraged to observe official Academy School social media profiles in an appropriate and safe way, for example, via a feed on the Academy's/School's website.

Any communication received by staff from children on any personal social media sites must be reported to the Designated Safeguarding Lead (DSL). In addition, if any member of staff is aware of any inappropriate communications involving any child in any social media, these must immediately be reported as above.

Social Media Platforms

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and 17 expects all staff and volunteers to share this commitment.

- The Academy School may have their own social media pages (such as Facebook, Instagram, X etc.), that they use as a tool to inform parents of significant events and successes of the Academy School
- The social media pages will be published, updated and monitored by the trust
- To safeguard everyone at the Academy School there are strict procedures in place regarding the use of the Academy School's social media pages
- The Academy School will **NEVER** post content which identifies any child or parent without permission.
- The Academy School will immediately remove any posts, which identify, name or compromise the privacy of any child or parent/carer who did not give their consent.
- Users are required to be polite and courteous in their communications. Any comments which are deemed to be inappropriate will be removed
- Users who repeatedly breach the guidelines will be banned from the page
- Should the Academy School have a social media page and SLT feel that the page is causing adverse or negative reflections of the Academy School, or that the site is burdensome to monitor and control, the page will be unpublished and/or deleted
- Staff wishing to use personal social media accounts should take every necessary precaution to avoid their professional reputation or the reputation of the Academy School being compromised in any way
- Personal social media accounts should not have any information data or photographs of Academy School children on their account
- Personal social media accounts should not be used during Academy School working times
- Concerns about inappropriate content/conduct in relation to a social media page, should be immediately reported to the Headteacher/DSL, in line with the Acceptable Use Agreement

Academy School Website - Published content

- The Headteacher/Principal takes responsibility for content published to the Academy School website but delegates general editorial responsibility to a designated member of office staff who are responsible for the editorial control of work provided for publication
- The Academy School will hold the copyright for any material published on their website or will obtain permission from the copyright holder prior to publishing with appropriate attribution
- The Academy School encourages the use of e-mail to contact the Academy School via the office
- The Academy School does not publish any contact details for the pupils

Safe Use of Images

- All digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official Academy School systems. Staff should not communicate with parents, carers or students through any personal accounts on social media platforms
- Photographs and videos of children may be taken for use in the Academy School using **only** Academy School equipment. Parental consent will be obtained before any image of a child is used on displays, the Academy School website or for use in media and press relations
- On entry to the Academy School, all parents must sign a permission slip for their children's images to be used on displays and the Academy School website

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and 18 expects all staff and volunteers to share this commitment.

- Use of images in media and press relations are discussed with parents on a needs basis
- Parents/carers are allowed to take photographs/video during Christmas plays and other Academy School events. However, it is made explicitly clear that these images **SHOULD NOT** be posted to social media sites
- Staff and children are not permitted to carry or use personal mobile devices during Academy School hours

Storage of Images

Images/ films of children are stored securely on the Academy School server and / or teacher's individual Academy School iPads

Complaints

Complaints or concerns relating to E-Safety should be made to the Headteacher/ Principal or the E-Safety coordinator. Incidents should be logged on the Online Safety Incident log (see Appendix 1).

Inappropriate material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Headteacher/Principal/E-Safety coordinator.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/Principal. Staff are aware that misuse or misconduct could lead to disciplinary action.

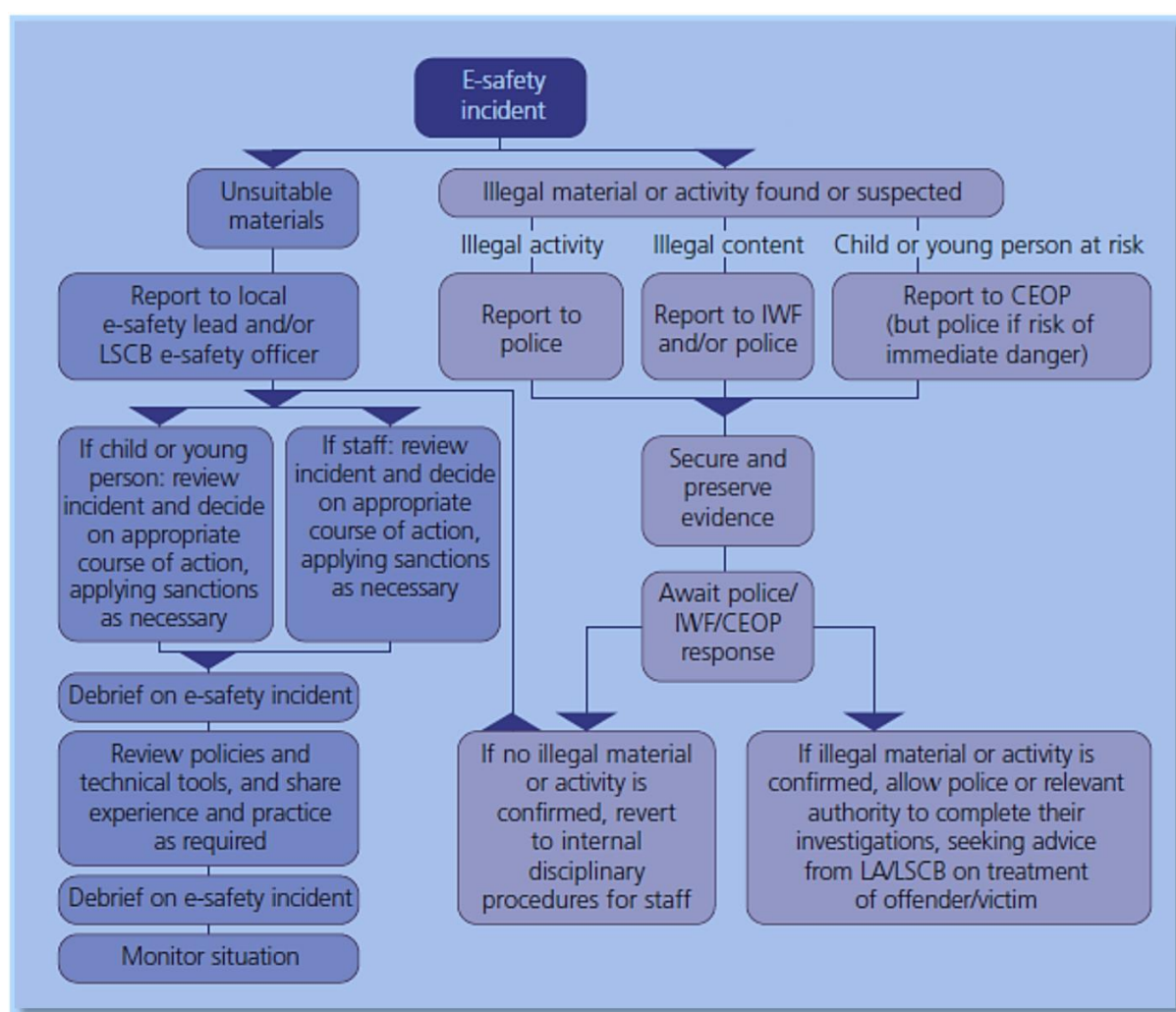
The Academy School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the Academy School network. The Academy School cannot accept liability for any material accessed, or any consequences of Internet access.

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and 19 expects all staff and volunteers to share this commitment.

Chancery Education Trust – Data Security, E-Safety Policy & Acceptable Use Agreement – September 2025



E-Safety Incident Flow Chart



Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and 20 expects all staff and volunteers to share this commitment.

Chancery Education Trust – Data Security, E-Safety Policy & Acceptable Use Agreement – September 2025



Useful Policies and Links

- Anti-bullying Policy
- Child Protection and Safeguarding Policy
- Staff Disciplinary Policy
- Personal Data Breach Policy
- Home Working Policy
- Mobile Device and Smart Technology Policy
- POSH: Professionals Online Safety Helpline- www.saferinternet.org.uk
- CEOP: Child Exploitation and Online Protection – www.ceop.police.uk
- IWF: Internet Watch Foundation – www.iwf.org.uk
- Facebook: Reporting a violation – www.facebook.com/help
- Truevision: Stop Hate Crimes – www.report-it.org.uk

Monitoring and Implementation Policy

The policy is reviewed annually, although the Trust may vary or amend it periodically to ensure that we fulfil our obligation around the Data Security, E-Safety Policy & Acceptable Use Agreement. All proposed changes to this policy would be made following the approval from the Committee.

	Name	Date
Policy written by	CET Board/Judicium	September 2025
Review by Committee	CET Board/Judicium	September 2025
Approved by Committee	CET Board	December 2025
Adopted by Governing Board	Local Governing Board	February 2026
To be reviewed annually		
Review by	September 2026	

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Chancery Education Trust – Data Security, E-Safety Policy & Acceptable Use Agreement – September 2025

Appendix 1

Online Safety Incident Log

Details of ALL online safety incidents are to be recorded by the E-Safety co-ordinator and passed to Headteacher/Principal to review. Serious incidents must be escalated immediately to the Headteacher/Principal/DSL

Date and Time	Name of Pupil/Staff Member	Room and Computer Device Number	Details of Incident (Include any evidence) Actions and Reasons	Actions and Reasons

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Appendix 2

Acceptable Use of Online Services by students and staff.

This agreement covers the use of all digital technologies in the Academy School: i.e. PC's, laptops, tablets, e-mail, internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

The use by staff and monitoring by the Academy School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner.

- I will follow the guidelines in the E-Safety policy (including mobile and handheld devices)
- I will only use the Academy School's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Headteacher/Principal and Local Governing Board
- I will not reveal my password(s) to anyone
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it
- I will not allow unauthorised individuals to access e-mail / Internet / intranet / network / VLE or other Academy School systems
- I will not engage in any online activity that may compromise the Academy School or my professional responsibilities
- I will only use the Academy School approved e-mail system for any Academy School business, including communication with parents. I will only enter into communication regarding appropriate Academy School business
- I will not browse, download or send material that could be considered offensive to anyone
- I will report any accidental access to, or receipt of inappropriate materials, or any filtering breach or equipment failure to the subject leader
- I will not download any software or resources from the Internet that can compromise the network or is not adequately licensed, or which might allow me to bypass filtering and security systems
- I will check copyright and not publish or distribute any work, including images, music and videos, that is protected by copyright, without seeking the author's permission
- I will not connect any device (including USB flash drives) to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the Academy's/School's anti-virus and other ICT 'defence' systems
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Chancery Education Trust – Data Security, E-Safety Policy & Acceptable Use Agreement – September 2025



- I will only use Academy School approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the staff shared work area of the Academy School network
- I will ensure that a senior member of staff is aware that the Academy School's photography/image equipment is being used and for what purpose
- I will follow the E-Safety policy on use of mobile phones / devices at the Academy School
- I will not use my personal photographic /video equipment, nor take images of children and young people using my personal mobile telephone
- I will use the Academy School's Learning Platform in accordance with Academy School protocols
- I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role
- I will ensure, where used, that I know how to use any social networking sites / tools securely, so as not to compromise my professional role
- I agree and accept that any computer or laptop loaned to me by the Academy School is provided solely to support my professional responsibilities, and that I will notify the Academy School of any "significant personal use", as defined by HM Revenue & Customs.
- I will only access Academy School resources remotely (such as from home) for example Arbor and follow e-security protocols to interact with them
- I will ensure any confidential data relating to children, the staff or the Academy School is not taken off site
- I understand that Data Protection policy requires that any information seen by me with regard to staff or pupil information that is held within the Academy School's information management system will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority
- I will alert the Academy School's DSL/DDSL/Headteacher/Principal if I feel the behaviour of any child or adult may be a cause for concern
- I will only use the Academy School network and Internet access in accordance with its policies
- I understand that it is my duty to support a whole-Academy School safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to the DSL/DDSL/Principal at the Academy School
- I understand that all Internet usage and network usage can be logged, and that this information can be made available to the DSL/DDSL/Headteacher/Principal on their request
- I will embed the Academy School's E-Safety/digital literacy curriculum into my teaching
- I understand that must adhere to the Academy School's AI (Artificial Intelligence) Policy

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Chancery Education Trust – Data Security, E-Safety Policy & Acceptable Use Agreement – September 2025



Agreed Sanctions as defined in the E-Safety policy

Staff

Incidents:	Refer to line manager	Refer to Principal/HT	Refer to HR	Refer to Police	Refer to Technical Support	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X		X			X
Inappropriate use of the internet / social media / personal email / AI	X	X	X				X
Personal use of the internet / social media / personal email	X	X	X				X
Unauthorised downloading or uploading of files	X	X	X		X		X
Allowing others to access the Academy School network by sharing username and passwords or attempting to access or accessing the Academy School network, using another person's account	X	X	X		X		X
Careless use of personal data eg holding or transferring data in an insecure manner	X	X	X				X
Deliberate actions to breach data protection or network security rules	X	X	X		X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X		X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X		X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X	X			X
Using personal devices for taking, editing and transferring images or videos of pupils of staff and storing any such images or videos at home	X	X	X	X			X
Actions which could compromise the staff member's professional standing	X	X	X				X
Actions which could bring the Academy School into disrepute or breach the integrity of the ethos of the Academy School	X	X	X			X	X
Using proxy sites or other means to subvert the Academy's/School's filtering system	X	X	X			X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X		X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X		X	X
Breaching copyright or licensing regulations	X	X	X				X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X		X	X

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

User Agreement

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and that I read and understand the Academy School's most recent E-Safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

I will sign the Policy Acknowledgement Form supplied via an online acknowledgment form.

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Chancery Education Trust – Data Security, E-Safety Policy & Acceptable Use Agreement – September 2025



Appendix 3



Pupil Acceptable Use & E-Safety Agreement

All pupils use computer facilities including internet access as an essential part of learning, as required by the National Curriculum. Pupils are asked to sign to show that the Acceptable Use and e-Safety rules have been understood and agreed.

Use of Computers in the Academy School

The Academy School owned equipment and network must be used appropriately

- ✓ The computer system is available for educational use only
- ✓ I will only log on with my own username and password
- ✓ I understand the Academy School monitors use of the information systems
- ✓ Printing – I will make sure my work is finished and checked and only print when instructed to do so
- ✓ I will take care when using the equipment so as not to cause damage
- ✓ If I do not follow these rules then I might have to speak to my Head of Year or my parents/carers might have to talk to the Headteacher/Principal about what I have done

These rules help us to stay safe on the Internet:

- ✓ I ask permission before using the Internet
- ✓ I only use websites that an adult has chosen or helped me choose
- ✓ I tell an adult immediately if I see or read anything I am uncomfortable with and switch my screen off
- ✓ I send emails that are polite and friendly
- ✓ I never give out personal information about myself or others or passwords
- ✓ I never arrange to meet anyone I don't know
- ✓ I do not open emails sent by anyone I don't know
- ✓ I do not use Internet chat rooms
- ✓ I am not allowed to connect personal devices to the Academy School network
- ✓ I will only post content online if it is appropriate and I have permission

This sheet can be kept at home for discussion as necessary

Pupil Acceptable Use & E-Safety Agreement - Page 1

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Chancery Education Trust – Data Security, E-Safety Policy & Acceptable Use Agreement – September 2025



This sheet is to be printed off, signed and returned to the Class Teacher/Academy School Office.

[ENTER ACADEMY SCHOOL NAME]

Pupil Acceptable Use & E-Safety Agreement

Pupil's Agreement

I have read and I understand the Academy School Acceptable Use and E-Safety Rules.

I will use the computers, network, Internet, email (with permission) and other new technologies in a responsible way at all times.

I know that my network, Internet and email use may be monitored.

Childs Name (Print)	
Class	
Year	

Parent's Agreement

Name (Print)	
Signature	
Date	

Pupil Acceptable Use & E-Safety Agreement - Page 2

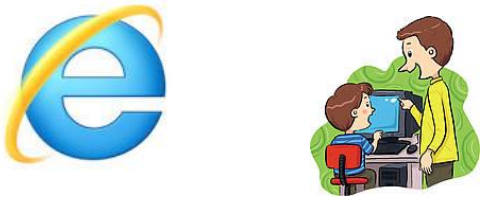
Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Chancery Education Trust – Data Security, E-Safety Policy & Acceptable Use Agreement – September 2025



Appendix 3

PUPIL ACCEPTABLE USE AGREEMENT FOR INFANT & NURSERY PUPILS

	
I will use the internet with an adult	I will only use programmes an adult says are safe
	
I will be friendly and polite when I use the computer	I will use my own password and username to login when using school technology.
	
I will tell an adult if I see something I do not like	I will keep my login and password private
	
I will only access the internet through the Impero app when using the school Ipads	I will always log out when I have finished using the internet on Impero

Signed: _____ (Child)

Class: _____

Date: _____

Chancery Education Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Chancery Education Trust – Data Security, E-Safety Policy & Acceptable Use Agreement – September 2025

