CAST Angling Project
Cornerstone House, Tilford Road,
Newstead Village, Nottingham NG15 0BU

CAST Angling Project – Acceptable Use of Technology and E-Safety Policy

Reviewed on 19th August 2025
To be reviewed on 18th August 2026

Contents

Introduction

In the 21st Century, ICT (Information and Communication Technology) is an essential resource to support both learning and teaching. It also plays an important role in the everyday lives/duties of children, young people, and adults. As a result, Education Providers are required to incorporate the uses of these technologies to arm our young learners with the skills to access life-long learning and employment.

Equally, Education Providers have a duty to ensure that this is done safely. This involves educating learners on the importance of staying safe online and the associated responsible use of technology.

This policy must be read in conjunction with the CAST Safeguarding and GDPR (2025) Policy.

Aims of the Policy

- To establish the CAST ground rules for using technology.
- To describe how these ground rules would fit into the wider context of other relevant policies, such as Safeguarding, Code of Conduct, Behaviour, etc.
- To demonstrate the methods used to protect children from sites containing material deemed inappropriate or harmful. This may be because the content is pornographic, sexually explicit, violent, extremist or radicalising, or discriminatory on the grounds of any of the 9 protected characteristics in the Equality Act 2010.

Information and Communications Technology covers a wide range of resources, and it is important to recognise the constant and fast-paced evolution of ICT within our society as a whole. Currently, the internet technologies that children and young people are using, both internal and external to the classroom, include:

- Websites.
- Apps.
- E-mail, instant messaging and chat rooms.
- Social media, including Facebook and Twitter.
- Mobile/smart phones with text, video and/or web functionality.
- Other mobile devices, including tablets and gaming devices.
- Online games.
- Learning platforms and virtual learning environments.
- Blogs and wikis.
- Podcasting.
- Video sharing.
- Downloading.
- On demand TV, video, films and radio/smart TVs.

Whilst exciting and beneficial both within and out of the context of education, most ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks and responsibilities associated with the use of these Internet technologies. At CAST, we understand the responsibility to educate our pupils on E-Safety Issues, teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using all forms of technology.

Technology Covered in this Policy

This policy (for all staff, regular visitors, parents (for regulated activities), and pupils) is inclusive of both fixed and mobile internet – the technologies provided by CAST (PCs, laptops, mobile devices, digital video equipment, etc.) and technologies owned by pupils and staff.

Background (Definitions)

Definition of Safeguarding:
Safeguarding children and protecting them from harm is the responsibility of everyone. All who come into contact with children and families have a role to play. The following is the accepted definition of 'safeguarding' and the promotion of wellbeing for children:

- Protecting children from maltreatment.
- Preventing impairment of children's health or development.
- Ensuring that children grow up in circumstances consistent with the provision of safe and effective care.
- Taking action so as to enable children to have optimum life changes, enter adulthood successfully, and have the best outcomes.

Local authorities/Education Providers have overarching responsibilities for safeguarding and promoting the welfare of all children and young people in their area. They have a number of statutory functions under the 1989 and 2004 Children Acts which make this clear.

This includes specific duties in relation to children in need and children suffering, or likely to suffer significant harm, regardless of where they are found, under sections 17 and 47 of the Children Act 1989.

Further information on this can be found in CAST Safeguarding Policy.

Definition of E-Safety:
In addition to the definition set out in the above, the term E-Safety is specifically defined for the purposes of this document in terms of limiting the risks to children and young people when using Internet, digital, and mobile technology (IDMTs).

CAST's vision is that all children, parents/carers, and all those working with children:

1. Recognise these risks and potential dangers that may arise from the use of technology in all forms.
2. Understand how to mitigate these risks.
3. Are able to recognise, challenge, and respond appropriately to any E-Safety concerns so that children are kept safe.

Potential Risks

We have a greater understanding of the extent of day-to-day dangers the virtual world can pose to children, which are including but not limited to:

- Being groomed online by adults, with the ultimate aim of exploiting them sexually.
- Being bullied by others via social networking sites (cyberbullying).
- The taking of inappropriate/indecent images of children which are then uploaded and circulated via websites or networking sites. This is a criminal offence under S45 of the Sexual Offences Act.
- The exposure of children to inappropriate/indecent/harmful images or material – including violence, sexual content (including pornography), and content that is discriminatory on the grounds of race, gender, sex, religion, disability and/or sexual orientation.
- Being exposed to the glorification and promotion of gang culture through gang websites, chat rooms, and forums.
- The targeting of children by groups wishing to radicalise children online through content that appears on websites, chat forums, or direct contact such as email or social media.

Ignoring these dangers would be a breach in our responsibilities in Working Together to Safeguard Children December 2023.

E-Safety Complaints

Please follow the CAST Complaints Policy.

We make every effort to resolve low level issues internally, and these are recorded locally.

All factors in relation to the complaint must be clearly established in order to have substance. Complaints about an employee's IDMT misuse should be escalated to the Safeguarding Officer and Directors immediately and be managed according to our Safeguarding Children Policy. We have the ability to scrutinise IDMT (Institute of Digital Media Technology) use in particular, and to identify sites accessed. Potentially illegal issues must always be referred to the police in the first instance.

Section 1 – Keeping Children and Young People Safe in Education and Learning.

CAST provide internet access to children through Student Wi-Fi access to assist with coursework. Our student Wi-Fi has an age restriction blocker and individual sites blocked for students' safety. Staff can switch off student Wi-Fi if there are any concerns.

Throughout the CAST SMSC curriculum and class workshops, all pupils are taught about the risks and responsibilities, as well as the educational rewards of using technology.

Pupils are taught to:

- Be cautious about the information given by others on such websites, for example, users not being who they say they are.
- Avoid placing images of themselves (or details within images that could give background detail) on such websites and to consider the appropriateness of any image they do post.
- Avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/home phone numbers, school details, IM/email address, specific hobbies/interests).
- Set and maintain their online profiles to maximum privacy and deny access to unknown individuals.
- Be wary about publishing specific/detailed private thoughts and information online.
- Report any incidents of cyberbullying to the school
- Be aware of the age restrictions on many social media applications (usually 13+).

Filtering

Levels of internet access and supervision must be appropriate and suitable for the children – however we recognise that there may be websites that staff may wish to access for research that might normally be filtered out, such as google images. Access controls (filtering) fall into several categories.

If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the E-Safety coordinator or teacher as appropriate.

Illegal Downloading

Children are made aware that if they attempt to download copyright protected files they are breaking the law of infringing intellectual property rights.

Cyberbullying

Cyberbullying is defined as the act of using the internet, mobile phones, video games, or other technology gadgets to send texts or post material intended to hurt or embarrass another person. "It is also defined as acts of aggression through computers, mobile phones and other electronic devices" (Jackson & Cohen, 2012).

At CAST, we have a zero-tolerance policy on this kind of behaviour. The law gives schools/Alternative Provisions the power to intervene in such cases, even when they have happened outside of school time (using technology that is not schools).

Those who participate in online bullying often use groups of friends to target their victims. An action intended as innocent could rapidly spiral out of control and young people may not realise that their actions constitute bullying.

The following are the most commonly reported types of cyberbullying:

- Email - can be sent directly to an individual or group to encourage them to participate in the bullying and can include derogatory comments or harassment.
- Instant Messaging (IM) – messages can be sent directly to an individual or group who can then be included in the conversation.
- Social networking sites – anonymous profiles can be set up to make fun of someone and each person contributing to these pages can soon worsen the problem.
- Inappropriate and threatening comments and images can be posted and circulated without consent.
- Mobile phones – anonymous and abusive text or video messages, photo messages, and phone calls can be shared via phones. This includes the videoing and sharing of physical or sexual attacks (a criminal offence) on individuals.
- Interactive gaming – games consoles allow users to chat online with anyone.
- Abuse of other online game players and the use of threats.
- Hacking into the account of another user for malicious reasons.
- Sending viruses – these can be sent from one person to another in order to destroy computers or delete/copy personal information from their hard drive.
- Abusing personal information – personal/sensitive information (including photographs and videos) being uploaded onto the internet without the victim's permission.

Some instances of cyberbullying do escalate into physical bullying. We take all instances of cyberbullying extremely seriously and we record all instances that are reported to us. We will escalate concerns to the police where necessary.

We encourage children to store the electronic records of abuse which will be essential in any subsequent investigation.

Monitoring E-Safety Incidences and Reporting Abuse

Any form of electronic or digital abuse (as defined in our child protection policy) will be reported to the CEOP service (www.ceop.police.uk), alongside the Director and Safeguarding Officer.

Any incidences which place a young person in immediate danger will be reported to 999.

We monitor E-Safety incidences, which is crucial for establishing any patterns and subsequently learning lessons quickly (see Appendix A)

CAST will liaise with Schools/LEA children's safeguarding board (guidelines given by schools) to ensure that we record the following:

- A description of the E-Safety incident.
- Those involves.
- How the incident was identified.
- What actions were taken and by whom.
- Conclusion of the incident.
- Lessons learnt – to inform the ongoing Policy and practice.

Pupils Sending Emails

No pupils at CAST are able to send emails within the provision.

Pupils are introduced to email as part of the Computing Programme of Study within schools and they may only: (1) use school-approved accounts on the school system, (2) be only under direct teacher supervision for educational purposes and (3) send emails only within their own schools. No email communication via the child can be sent to CAST due to GDPR regulations.

Pupils and Mobile Phones

Pupils are allowed to bring personal mobile devices/phones to CAST but must not use them for personal purposes within lesson time. At all times the device must be turned off or put on silent mode and handed in if affecting their or others learning. CAST is not responsible for the loss, damage or theft of any personal device or mobile phone. Users bringing personal devices into CAST must ensure there is no inappropriate content on the device.

Pupils with Additional Needs

CAST endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the CAST E-Safety rules. However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Staff's internet activities are planned and well managed for these children and young people.

Involving Parents and Carers

At CAST we believe that it is essential for parents/carers to be fully involved with promoting E-Safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss E-Safety with parents/carers and seek to promote a wide understanding of the benefits of new technologies, together with associated risks.

Parents/carers are required to make a decision as to whether the consent to images of their child being taken and used in the public domain (e.g., on CAST website or Facebook page), information to parents relating to E-Safety where appropriate will be in the form of posters, website information, and CAST community newsletter items.

Section 2 – Keeping Adults Safe

As well as a duty to keep children safe, CAST also takes seriously its duty to protect adults regarding the use of technology in the workplace. As such we ask that all adults read and sign a copy of the Managing Allegations in Education Policy, Lone Working Policy, and GDPR Policy. Staff training for raising awareness on E-Safety and Data Protection awareness is initiated within the academic year.

Monitoring

All monitoring, surveillance or investigative activities are conducted by CAST designated ICT support staff and comply within the GDPR Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA), the Lawful Business Practice Regulations 2000 and from June 2025 The Data Use and Access Act 2025 (DUAA). (The DUAA amends, but does not replace, the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulations (PECR).)

Personal Data

CAST holds personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can potentially damage the reputation of CAST. Everybody in the school community has a shared responsibility to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

GDPR enhances the protection of children's personal data. Any privacy notices for services offered directly to a child must be written in clear, simple language and to be taken as valid.

New GDPR regulations of 2018 have key areas of changes; the most significant changes that will affect how we all work is in additional rights afforded to individuals. These allow individuals to request access, corrections and removal of their personal information in ways that weren't available before.

Individuals have rights and responsibilities under the new GDPR regulations which CAST adhere to and can respond to requests.

Six principles of processing personal data are depicted in the GDPR 2018 Legislation – see CAST GDPR Policy/CAST Deletion Policy on how we meet these guidelines.

From **June 2025** The Data Use and Access Act 2025 (DUAA) amends, but does not replace,
The UK General Data Protection Regulation (UK GDPR),
The Data Protection Act 2018 (DPA) and
The Privacy and Electronic Communications Regulations (PECR).)

INSERT NEW SECTION AND CHECK REST OF POLICY

Breaches

The new regulation requires clearer evidence of consent from individuals and some methods of recording consent will no longer be valid. Additionally , GDPR gives greater powers to the ICO (Information Commissioner's Office) to investigate organisations and breaches.

A breach or suspected breach of policy by a CAST employee, contractor or pupil may result in the temporary or permanent withdrawal of CAST's ICT hardware, software or services from the individual concerned.

For staff any policy breach is grounds for disciplinary action in accordance with the CAST Disciplinary Procedure or, for support staff, in their probationary period as stated. Incidents will be reported to the GDPR Officer and senior staff.

Policy breaches may also lead to criminal or civil proceedings. See the GDPR Policy relating to security breaches.

Staff Sending Emails

The use of email within CAST is an essential means of communication for both staff and partnership schools. For this reason, it is important that all staff check their email regularly, to ensure email archives are to a minimum. In the context of school, email should not be considered private. Educationally, email can offer significant benefits and we recognise that pupils need to understand how to use email in relation to their age and how to behave responsible online. All using Password Protected Security emails in relation to pupil’s data. Abbreviations for some names will be used. An audit for GDPR ensures all contact information is relevant and current. See CAST GDPR/Deletion Policy.

Managing Emails

CAST gives some staff their own email account (not all Tutors have access to a general email used for those purposes for general concerns) and for other related CAST business. Administration, Safeguarding Officer, Directors and Finance Manager have own accessible emails.

This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal information being revealed. Archived information from emails is kept on a hard drive to ensure current and up to date information is kept under new GDPR regulations. Staff should use their school email for all professional communication. It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary, email histories can be traced. Staff should not contact pupils, parents or conduct any school business using personal email addresses.

A CAST audit for GDPR ensures all contact information is relevant and current and reviewed and updated regularly. Archived information is kept on a hard drive. See the CAST GDPR/Deletion Policy.

The school requires a standard disclaimer to be attached to all email correspondence, stating that, ‘the views expressed are not necessarily those of the school or LA’.

Staff must inform the DPO (Data Protection Officer) if they receive an offensive email. Any emails created or received as part of the job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your email account as follows:

- Organise email into folders and regularly delete old/unwanted mail.

- Emails containing personal, confidential, classified or financially sensitive.
- Data sent to external third parties or agencies should be marked as confidential (refer to the Section ‘Emailing personal, sensitive, confidential or classified information).
- Use only your own CAST email account (not that of other staff members)
- Do not send/forward attachments internally unnecessarily.
- Do not use CAST email for personal business.
- Never open attachments from untrusted sources; consult your network manager/Admin first.
- Be aware that CAST based email and internet activity can be monitored and explored further if required.

Emailing Personal, Sensitive or Confidential/Classified Information

Where email must be used to transmit/process such data:

- Obtain consent from your manager to provide the information by email.
- Verify the details, including accurate email address of any intended recipient.
- Verify (by phoning) the details of a requestor before responding to email requests for information.
- Do not copy in or forward emails to any more recipients than necessary.
- Do not send the information to any person whose details you have been unable to verify.
- Send the information as an encrypted/password protected document attached to the email.
- Provide the encryption key or password by a separate email/contact with the recipient(s).
- Do not identify such information in the subject line of any email.
- Request conformation of safe receipt.

Personal Mobile Devices (Including Mobile Phones)

Staff are permitted to bring in personal mobile phones and devices for their own use. Under no circumstances should a member of staff contact a pupil or parent/carer using their personal device. They must not use it to take video footage or still images of pupils or any other school activity. Under GDPR contacts for parents/students should be called via the main office or on a designated work phone.

CAST provide Tutors with in-house mobile phones to ensure data protection regulations are met. Mobile phones are not allowed to be used by staff in classrooms. The sending of inappropriate text messages between any member of the school community is not allowed.

CAST is not responsible for the loss, damage or theft of any personal mobile device of staff. Users bringing personal devices into CAST must ensure there is no inappropriate or illegal content on the device.

CAST-Provided Mobile Phones

Devices provided by CAST must only be used for educational business and are subject to the same rules when being used offsite. Permission must be sought before any image or sound recordings are made on the devices of any member of the CAST community. Where CAST provides mobile technologies such as phones for offsite visits and trips, only these devices should be used.

Pupil and staff emergency contacts are kept within the main office and are given to staff via phone to contact parent/carers/schools, these are then deleted from the phone to ensure GDPR data protection regulations are met.

Use of Social Media

Facebook, Twitter, Instagram, Snap Chat and other forms of social media are increasingly becoming an important part of our daily lives. CAST uses its own website, Instagram and Facebook but with parental consent if names and photos are used on the site. This is another way CAST try to communicate with parents and carers.

In relation to social media, the following applies:

- Staff are not permitted to access their personal social media accounts using CAST equipment at any time when they are ‘in loco parentis’ (usually from 8:00am – 4:30pm).
- Staff, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.
- Staff, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others and copied.
- Staff, pupils, parents and carers are aware that their online behaviour should at all-time be compatible with UK law.

Use of Land Line Telephones

CAST telephones are provided specifically for business purposes. Personal usage is a privilege that will be withdrawn if abused. Staff may make or receive personal telephone calls provided:

- They are infrequent, kept as brief as possible and do not cause annoyance to others.
- They are not for profit.
- They are not to premium rate services.

Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases.

Ensure that your incoming/outgoing calls do not interfere with your duties within work or primarily learning and teaching. Any telephone calls during teaching time should be in the event of an emergency only. Follow the appropriate procedures (Emergency Contingency Plan) in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout the office.

Keeping Data and Equipment Protected

Computer Viruses

- All files downloaded from the internet, received via email or other means must be checked for viruses using CAST provided anti-virus. This also includes files downloaded from memory sticks and external hard drives.
- Never interfere with any anti-virus software installed on CAST ICT equipment. Always update when prompted to do so.
- If your machine is not routinely connected to the CAST network, you must make provision for regular virus checks through the IT support team.
- To prevent vulnerability of viruses on the system, keep the windows program up to date and install optional updates if prompted to do so.
- If you suspect there may be a virus on any CAST ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

Data Security

The accessing, processing, and storing of data and the appropriate use of CAST data is something we take very seriously. CAST give relevant staff access to its Management Information System, with a unique username and password and it is the responsibility of everyone to keep passwords secure. All staff are aware of their responsibility when accessing CAST data and have been issued with relevant guidance documents and the Policy for GDPR/Deletion.

All staff should:

- Keep all CAST related data secure. This includes all personal, sensitive, confidential or classified data.

- Avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked and out of sight.
- Be responsible to ensure the security of any personal, sensitive, confidential and classified information contained in documents that are copied, scanned or printed.
- Notify the recipient before sensitive/confidential messages are sent.
- Read all relevant policies in line with this policy.

All staff agree to:

- Ensure that any CAST information accessed from your PC or removable media equipment is kept secure and remove any portable media from computers when not attended.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access.
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others.
- Ensure that personal, sensitive confidential or classified information is not disclosed to any unauthorised person.
- Only download personal data from systems if authorised to do so by your manager.
- Not to post on the internet personal, sensitive, confidential or classified information, or disseminate such information in any way that may compromise its intended restricted audience.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling.

Passwords and Password Security

- Always use your own personal passwords or ones given to you by the IT admin.
- Make sure you enter your personal password each time you log on and do not save passwords in any automated logon procedures.
- Staff should change temporary passwords at first logon
- Change passwords immediately whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- Only disclose your personal password to authorised ICT support staff when necessary and never anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- Never tell a child or colleague your passwords.

Relevant Responsible Person

Senior members of staff should be familiar with information risks and the CAST's response. The senior leadership team (Directors/QA Lead/DPO) have the following responsibilities:

- To lead on the information risk policy and risk assessment.
- To advise staff on appropriate use of CAST technology.
- To act as an advocate for information risk management
- What information is held, and for what purposes.
- What information needs to be protected, how information will be amended or added/deleted.
- Who has access to the data and why.
- How information is retained and disposed of.

For information such as assessment records, medical information and special educational needs data, a responsible member of staff will identify passwords across the provision as and when needed.

As a result, Managers are able to address risks to the information and make sure that information handling complies with legal requirements. However, it should be clear to all staff that handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Disposal of Redundant ICT Equipment

All redundant ICT equipment will be disposed of. All redundant ICT equipment that may have help personal data will have the storage archived onto a hard drive or erased in line with the Deletion Policy. This is to ensure the data is irretrievably destroyed. If the storage media has failed it will be physically destroyed. We will securely dispose of removable media that may hold personal data. It is essential that any hard drives which may have help personal data or confidential data are 'scrubbed' in a way that means data can no longer be read. It is not enough to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a written guarantee that they will irretrievably destroy the data.

Disposal of any ICT equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006. The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Data Protection Act 1998. Electricity at Work Regulations 1989.

The provision will maintain a comprehensive inventory of all its ICT equipment including a record of disposal which will include: (In line with any GDPR requirements)

- Date and item disposed of.
- Authorisation for disposal.
- Verification of software licensing.
- Any personal data likely to be held on the equipment.
- How it was disposed of e.g., waste, gift, sale.
- Name of company/organisation/person who received the disposed item.
- Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the provision and therefore no longer have authorised access to the CAST systems. Such zombie accounts when left active can cause a security threat by allowing unauthorised access. CAST will ensure that all user accounts are disabled once a member of staff has left. Prompt action on disabling accounts will prevent unauthorised access.

Servers

- Always keep servers in a locked secure environment.
- Limit access rights.
- Always password protect and lock the server.
- Existing servers should have security software installed appropriate to the machine's specification.
- Backup should be encrypted by appropriate software.
- Data must be backed up regularly.
- Backup media stored off site must be secure.
- Remote backup should be automatically securely encrypted.

Review Procedure

There will be ongoing opportunities for staff to discuss with the E-Safety coordinator any E-Safety issues that concern them.
This policy will be reviewed every 12 months and consideration will be given to the implications for future development planning. The policy will be amended if new technologies are adopted or if Central Government change the orders or guidance in any way. E.g., amendments to GDPR.

Further Help and Support and Current Legislation/Acts

For further help and support, please visit: office – www.ico.org.uk – Data Protection.

The current Legislation that applies to acceptable uses of technology and e-safety are as follows. This includes material that might be criminal, cause harm to young people or be otherwise unlawful:

- The GDPR Act 2018
- The Data Use and Access Act 2025 (DUAA)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998
- Freedom of Information Act 2000 (Amendment) EU Exit Regulations 2018

Other acts relating to e-safety/data protection are:

- Racial and Religious Hatred Act 2006
- Sexual Offences Act 2003
- Communications Act 2003 (section 127)
- The Computer Misuse Act 1990 (sections 1-3)
- Malicious Communications Act 1988 (section1)
- Copyright, Design and Patents Act 1988
- Public Order Act 1986 (sections 17-29)
- Protection of Children Act 1978 (Section1)
- Obscene Publications Act 1959 and 1964/1999
- Protection from Harassment Act 1997
- Acts Relating to the Protection of Personal Data
- Data Protection Act 1998
- Criminal Justice Act 1988/2003

This policy was written in line with the GDPR regulations 2018
and The Data Use and Access Act 2025 (DUAA)

Appendix A

CAST Angling Project –
E-Safety Concern and Record of Action

This form is to be used to record any incidences of cyberbullying or inappropriate use(s) of technology that come to our attention, both internal and external to CAST.

Name of victim:…………………………………………………………………………

Tutor group:………………………………………………………………………..

Site:………………………………………………………………………………………

Date: ……………………………………………………………………………………..

Type of technology that has been misused: ……………………………………

Where is the technology located?

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

Incident description:

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

Full names of all involved (including year groups and sites):

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

How do we know about the incident? Who brought it to our attention?

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

What actions were taken and by whom?

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……..……………………………..……………………..………………..……………….….

Conclusion of the incident and lessons learnt – how was it dealt with and what could be done differently next time?

…………………..………………….…………..……………………..………………..………

……..………………..………………..…………………..………………..………………….…..

……..……………………………..……………………..………………..……………….….

…………………..………………….…………..……………………..………………..………

……..………………..………………..…………………..………………..………………….…..

……..……………………………..……………………..………………..……………….….

(To be completed by the E-Safety Lead/DSL/SLT/DPO)

Report completed by:…………………..…………………………..……………..…………...

Sign:……………………………………………..………………….............................

Date:……………………………………………..…………………............................

Signed as seen by DSL/DPO/SLT:………………………………………………..

Dear parent/carer,

ICT (Information and Communication Technology) including the internet, email, and mobile technologies has become an important part of learning in our provision. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these E-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation, please contact one of the staff at CAST.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/children and not deliberately upload or add any text, image, sound, or videos that could upset or offend any member of the school community. We will support our partner schools in the approach to provide online safety.

We have discussed this document with [Learner name]………………………….. and we agree to follow the E-Safety rules and support the safe use of ICT in and out of CAST.

Parent/carer signature:

Date:

Pupil Acceptable Use Agreement/E-Safety Rules

As a pupil at CAST I agree that:

- I will only use CAST ICT for educational purposes.
- I will make sure that all ICT contact with other students and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidently find anything like this, I will tell my tutor immediately.
- I will not give out my own / others details such as name, phone number or home address.
- I will not arrange to meet someone or send my image unless is part of a project approved by CAST.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me and others safe.
- I will support the CAST approach to online safety and not deliberately send or add any images, video, sound or text that could upset any member of the school community.
- I cannot access the internet at CAST. My own data will be used when I use my own phone in social times.
- I know that my use of ICT can be checked, and my parent / carer contacted if a member of staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a project approved by a CAST tutor.
- I will not use CAST technology for the purposes of private gaming.

I understand that if this happens, I will have my rights to CAST technology access withdrawn.

Student sign:…………………………………………………………………………

Student print name:………………………………………………………………

Date:………………………………………………………………………………

Internet Safety and Acceptable Use for Staff and Visitors to Sign.

In line with our policy on E-Safety/data protection it is requested that all those using technology within CAST, read and sign the agreement below:

Internet use

- Children and non-staff adults are not to use the internet without staff supervision.
- Any web pages to be used for teaching purposes should be screened by a member of staff before use with children.
- Fire walls, Anti-Virus, content screening software or service providers with filtering facilities are to be used wherever possible.
- Children and non-staff adults are instructed in the responsible use of the internet and are asked to report any unsuitable material directly to the DPO (Data Protection Officer) E-Safety Co-ordinator or a member of the Senior Leadership Team promptly.
- Unsuitable content which is not blocked via the CAST filtering system should be reported to the DPO and Senior Leadership Team promptly.
- The internet should be used for curriculum, professional and administration purposes only.
- No information which could lead to the unauthorised identification or contact of an individual child or adult by a member of the public may be published on the internet.
- Photographs of children may only be published on the CAST Facebook/website with parental permission but the children should never be named.
- Private contact details of staff or children (other than the school contact details) must not be published on the internet.

- The use of or viewing of online gambling sites are strictly forbidden.

Email Use

- Excessive unsolicited i.e. ‘Spam’ to be reported to a technology team member. Under no circumstances should any accompanying attachments be opened.
- Any school business should only be conducted via the CAST email system provided.
- Use of personal email accounts to conduct CAST business is not permitted and CAST email accounts should not be used for personal use.
- No personal email accounts may be accessed on ICT by staff. Personal use of email is not permitted.
- Personal use of email of students is not permitted.
- Personal use of email by visitors and those outside of CAST is not permitted, unless authorised by a senior member of staff.
- No information which could lead to the unauthorised identification or contact of an individual child or adult by a member of the public may be emailed.
- No photographs of children may be emailed via CAST email within the organisation freely. This must be authorised by a senior member of staff.
- Staff and guests should be instructed in the responsible use ICT facilities.
- Staff and guests must not interfere with the work of others on the system either directly or indirectly.
- Staff must be aware that CAST based email and internet activity is monitored and explored further if required.
- The facilities must be used in a responsible manner, in particular, staff and guests must not deliberately view, create or transmit material that is deemed / likely to be deemed as obscene, defamatory or indecent, cause annoyance, inconvenience, anxiety or offence. Or infringes the copyright of another person.
- Staff must ensure that they do not download viruses on CAST computer systems or networks.

If staff, students or guests are found to have infringed these guidelines, then the incident must be reported to the DPO and Senior Leadership Team as soon as possible and depending upon the severity of the incident, a verbal or written warning may be given; the user may be allowed only restricted access to facilities; the user may lose the privilege of using the facilities; or the initiation of staff disciplinary procedures may result, or, in extreme cases, the police may be contacted.

Use and Storage of Digital Images and Media

- Photographs and video taken of children must always be done using the CAST equipment, never using personal phones or cameras of staff or other individuals.
- When pictures are stored on the network, they should be deleted once used and should never be stored beyond their purpose. Exceptions to this would be for school purposes such as the CAST Newsletter, or photographs used for publication purposes/future units of study.
- Images of children at CAST should never be stored on home computers or other equipment.
- CAST cameras which hold images of children should not be taken outside of CAST unless of CAST business.
- WhatsApp group chat and messages are to be cleared on a regular basis.

I agree to the terms set out in this agreement. I understand that internet use and email use may be monitored.

I understand that if this happens, I will have my rights to CAST technology access withdrawn.

Signed:………………………………………………………………………………...

Print name:………………………………………………………………………

Date:………………………………………………………………………………