Non- Statutory

# Online Safety Policy

# TRINITAS ACADEMY TRUST

**This policy supports the Trinitas Principles as outlined below;**

*We will share responsibility for all of the children in all of the schools.*

*We will recruit high quality staff because the quality of Trinitas Academy Trust is determined by the quality of those who work within it.*

*We will value our staff by respecting their professional competence, through robust monitoring, challenge, and support and by rewarding them for their contribution to Trinitas Academy Trust.*

*We will ensure outstanding achievement for children and staff by being strategic, aspirational and not afraid to innovate.*

*We will teach our children through a curriculum that engages and motivates them, celebrates success, meets their individual needs and prepares them for the future.*

*We will provide the best possible learning environment, which is inspiring for both pupils and staff.*

*We will ensure that the systems within the Trust and the organisation of the Trust are coherent, robust and offer best value for money.*

*We will be wholly committed to promoting the Anglican Ethos of the Trust by being distinctive yet inclusive.*

*We will hold true to our values and aspirations, without compromise.*

**Policy Owner: Trust Safeguarding Lead**

**Aim: This policy fits within broader policies and it aims to have a complete and consistent approach to online safety within Trinitas Academy Trust and its schools.**

**Audience: All stakeholders**

**Copies are available: *Website and school office***

**Review 24 October 2018**

**Latest updates September 2019**

**Updated February 2020**

**Review Date: October 2021**

***Linked policies include:*** *Information and Information and Communication Technology Policy, Safeguarding & Child Protection Policy, , Behaviour Policy, Anti Bullying Policy and anti-racism strategy, Computing Policy,* Data Protection and GDPR Policy, *Health & Safety Policy Fair Prevent Policy, Information Technology Acceptable Use Policy, Records Management Policy Searching, Screening and Confiscation Policy, Sexual Violence and Harassment between Children Policy, Treatment at Work Policy, Visitors Policy, Whistle blowing Policy, Safer Recruitment,*

**QUALITY ASSURANCE**

*Trinitas Academy Trust will ensure that systems are in place to monitor the implementation of, and compliance with this policy and accompanying procedures. This will include periodic audits of online safety procedures and systems including record keeping of online safety incidents by the Trust's Safeguarding Leader and Designated Safeguarding Lead.*

*The individual school's Senior Leadership Team and the Governing Body will ensure that action is taken to remedy without delay any deficiencies and weaknesses identified in online safety arrangements.*

## *Policy Statement*

**Trinitas Academy Trust is committed to practice, which protects children from harm. Staff and volunteers in this organisation accept and recognise our responsibilities to develop awareness of the issues, which cause children harm.**

**Equality Statement**

Trinitas Academy Trust is committed to promoting equality and preventing discrimination on the grounds of disability, ethnicity, gender, age, religion, belief or sexual orientation.

**Contents**

***Appendices:***

## 1. Introduction

### Rationale

Trinitas Academy Trust acknowledges the value of using appropriate internet resources for Teaching and Learning and the necessity of using them for administrative purposes. The Trust acknowledges overlapping duties of care towards pupils and others, whether moral, or arising from Company, Charity, Education or Employment law.
As with other safety measures, the Trust aims to educate children to recognise and evaluate relevant danger and to adopt safe practices. This will always be underpinned with adult supervision appropriate to age and stage and may be aided by automated technologies for supervising and monitoring online activity. A safe communication climate is also encouraged which will enable policy and practice to adapt to experience.

### Scope (from SWGfL)

- This policy applies to all members of Trinitas Academy Trust community (including governors, staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the school's IT systems, both in and out of the school.

- The Education and Inspections Act 2006 empowers Head Teachers/Principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying, or other online safety incidents covered by this policy, which may take place outside of the schools but is linked to membership of the schools. The 2011 Education Act increased these powers with regard to the searching for electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the Behaviour Policy.

- The school will deal with such incidents within this policy and associated child protection, behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online behaviour that take place out of school.

**Acceptable User Policy**
All use of ICT facilities is governed by an Acceptable Usage Policy (AUP). All staff, Trustees, members of Local Governing Bodies, pupils and their parents, guardians or carers shall be made aware of the AUP in their induction; they must provide signed acknowledgement being allowed access.

- Acceptable Use Policy to be issued to the whole school community, usually on entry to the school.
- Acceptable Use Policy to be held in pupil and personnel files.
- Acceptable Use Policy to appear when staff or pupil log on to the schools computer systems.

## 2. Roles and Responsibilities

| Role | Key Responsibilities |
|---|---|
| **Principals/Head Teachers** | • Takes overall responsibility for online safety provision.<br>• Is the Data Controller for personal data that the school hold.<br>• Ensures staff read and sign that they have understood the school's online safety Policy.<br>• Responsible for ensuring that *all* staff receive suitable training to carry out their online safety roles and to train other staff, as relevant.<br>• Receives regular monitoring reports from the Designated Safeguarding Lead/Child Protection Officers.<br>• Ensures that there is a system in place to monitor and support staff who carry out internal online safety procedures. |
| **Senior Leader Team** | • Makes clear that all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through new staff inductions, staff meetings and teaching programme. |
| **Trust Operation Director** | **The Trust Operation Director is responsible for data control and oversees the development of a Data Protection Policy. They will:**<br>• Take overall responsibility for data and data security as the Data Protection Officer (DPO).<br>• Take ownership of the risk assessment process for information risk, including review of the annual information risk assessment to support and inform the Statement of Internal Control.<br>• Review and agree an action plan in respect of identified information risks.<br>• Ensure that the Trust's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.<br>• Provide a focal point for the resolution and/or discussion of information risk issues.<br>• Ensure the Governing Body is adequately briefed on information risk |

| | |
|---|---|
| | issues. |
| **Data Protection Officer (DPO)** | **The Trust Operations Director holds the role of DPO. He will have professional experience and knowledge of data protection law, particularly that in relation to the education system.**<br>**The DPO is appointed in order to:**<br>• Inform and advise the Trust, schools and its employees about their obligations to comply with the GDPR and other data protection laws.<br>• Monitor the Trust and school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.<br>• Report to the highest level of management at the Trust, which is the Chief Executive Officer. |
| **Designated Safeguarding Lead (DSL)** | **Takes day-to-day responsibility for online safety issues.**<br>• Is regularly updated in online safety issues and legislation, and is aware of the potential for serious child protection issues that could arise from:<br>➢ sharing of personal data<br>➢ access to illegal / inappropriate materials<br>➢ inappropriate online contact with adults / strangers<br>➢ potential or actual incidents of grooming<br>➢ online bullying and use of social media<br>• Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident by providing advice and information on reporting offensive materials, abuse/ bullying and is available for pupils, staff and parents.<br>• Promotes an awareness and commitment to online-safeguarding throughout the school community.<br>• Ensures that online safety incident logs are kept up to date.<br>• Facilitates training and advice for all staff.<br>• Communicates regularly with Senior Leader Team and the designated online safety Governor and committee to discuss current issues, review incident logs and filtering/change control logs.<br>• Will liaise with Trinitas Academy Trust IT Support.<br>• Will liaise with the Local Authority (LA) and relevant agencies when appropriate.<br>• Immediately refers any material they suspect is illegal to the appropriate authorities – Police – Child Exploitation and Online Protection (CEOPS) and the LA.<br>• Inform parents of any online safety concerns on social media or within the school. |
| **Governors / Safeguarding Governor** | **The Safeguarding Governor's responsibilities includes an overview of online safety.**<br>**All Governors are invited to take part in online safety training/awareness sessions.**<br>**The role of the Online Safety Governor will include:**<br>• Approve (with other school Governors) the online safety policy and review the effectiveness of the policy.<br>• Ensure that the school follows all current online safety advice to keep the pupils and staff safe.<br>• Receive information about online safety incidents and monitoring reports from the Designated Safeguarding Lead and Computer Subject Leader<br>• Monitor what pupils are learning through the curriculum in regards to |

| | |
|---|---|
| | online safety.<br>• Supports the schools in encouraging parents and the wider community to become engaged in online safety activities. |
| **Trinitas Academy Trust IT Support** | **Trinitas Academy Trust IT Support ensure the network is used safely and securely for the schools within the Trust and will report any online safety related issues that arise to the individual school's Designated Safeguarding Lead.**<br>**The management of our infrastructure will:**<br>• Keep up- to-date with the school's online safety policy.<br>• Ensure that our wired and wireless networks are secure.<br>• Manage network accounts and permissions for all pupils and staff.<br>• Inform all users that Internet use is monitored.<br>• Administer firewall and content filtering to role, age of pupil and key stage.<br>• Manage the School Information Management System (SIMs) account and permissions for staff.<br>• Limit email recipients and senders using school facilities to known safe groups, as appropriate to educational stage.<br>• Respond to requests from teaching staff to block, allow or review the classification of identified websites or pages.<br>• Regularly review security settings for all resources especially where personal data is involved.<br>• Investigate suspected systems abuse, promptly and vigorously.<br>• Take immediate steps to deny access to any person suspected of breaching the AUP if necessary and depending on severity.<br>• Require that all users log off or lock the computer when they have finished working or when leaving the computer unattended.<br>• Set-up the network so that pupils cannot download executable files/ programmes.<br>• Ensure Health and Safety is followed, while maintaining equipment, e.g. projector filters cleaned by site manager |
| **All staff** | • Read, understand and help promote the Trust's online safety policies and guidance.<br>• Read, understand, sign and adhere to the school staff Acceptable Use Policy.<br>• Be aware of online safety issues relating to the use of mobile phones, cameras and hand held devices and report any suspected misuse or problem to the Designated Safeguarding Lead.<br>• Model safe, responsible and professional behaviour in their own use of technology.<br>• Ensure that any digital communications with pupils should be on a professional level and only through school based systems, e,g school email access and Google G Suite and Classroom accounts.<br>**GDPR**<br>Before sharing data, staff should always ensure that:<br>• They have consent from data subjects to share it, if required.<br>• Adequate security is in place to protect it.<br>• The data recipient has been outlined in a privacy notice. |
| **Computing Subject Leader** | • Oversee the delivery of the online safety element of the school curriculum.<br>• Liaise with the Designated Safeguarding Lead regularly concerning any online issues or concerns.<br>• Liaise with Trinitas Academy Trust IT Support. |

| | |
|---|---|
| **Teachers and Teacher Assistants** | • Embed online safety issues in all aspects of the curriculum and other school activities.<br>• Supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant).<br>• Are vigilant in their supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.<br>• Will preview websites before use [where not previously viewed or cached]; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open internet searching is required; e.g. Google Safe Search, DIBDABDOO.com<br>• Ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright.<br>• Makes clear that no one should log on as another user. Pupils should never be allowed to log on or use staff logins as these have far less security restrictions and inappropriate use could damage files or the network.<br>• Must not log on as a pupil.<br>• Must log off after using the computer but must not shut the computer down in order that the system can apply updates. The computer will shut down at the end of the updates to save energy.<br>• Ensure that they store laptops and tablets each night in the rechargeable trolley and it is locked. |
| **Pupils** | • Read, understand, sign and adhere to the Pupil Acceptable Use Policy (NB: at **KS1** it would be expected that parents/carers would also sign the AUP agreement.<br>• Have an understanding of safe research skills and **'Stop and Think Before You Click'**.<br>• Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.<br>• Know and understand school policy on the use of personal mobile phones, digital cameras and hand held devices. (Bring Your Own Device - BOYD)<br>• To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings<br>• To understand acceptable behaviour when using an online environment / email, e.g be polite, no bad or abusive language or other inappropriate behaviour, keeping personal information private.<br>• To understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments;<br>• To develop a range of strategies to evaluate and verify information before accepting its accuracy.<br>• To understand why they must not post pictures or videos of others without their permission; for older pupils [e.g. Year 5] to understand why and how some people will 'groom' young people for sexual reasons.<br>• To understand the impact of online bullying, Sexting (Youth Produced Sexual Imagery) and trolling and know how to seek help if they are affected by any form of online bullying.<br>• To know how to report any abuse including online bullying; and how to seek help if they experience problems when using the Internet and related |

| | |
|---|---|
| | technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button. |
| **School Parliament/ School Council/School Online safety Committee** | • Conduct an online bullying assembly during Anti-Bullying week.<br>• To organise a special assembly on Safer Internet Days (SID).<br>• Assist teachers to monitor the online safety displays in the classroom and ICT suite, e.g. ensure that the SMART rules are on display.<br>• Take part in online safety parent workshops.<br>• Consult the views of other children and see if there are any concerns or issues they need to be aware of.<br>• Help the Computing Subject Leader and Designated Safeguarding Lead identify any areas of concern on social media use that they become aware of. |
| **Parents/carers** | • To support the school in promoting online safety and endorse the Parents' Acceptable Use Policy.<br>• Read, understand and promote the school Pupil Acceptable Use Policy with their children.<br>• Consult the school if they have any concerns about their children's use of technology.<br>• Raise queries, concerns or complaints directly with the school rather than posting them on social media.<br>• Should not post malicious or fictitious comments on social media sites about any member of the school community.<br>• Should not form online friendships or enter into online communication with employees, as this could lead to professional relationships being compromised, unless they are related. |

## 3. Communication:

The policy will be communicated in the following ways:

- The policy will be shared at a staff briefing.
- Pupils will be informed of the content through lessons and assemblies.
- The policy will be posted on the school websites.
- The policy is part of the schools induction pack for new staff.

## 4. Education and Curriculum

### Pupil online safety curriculum

Creating a culture that incorporates the principles of online safety across all elements of school life will be achieved through school's policies and practice and will be communicated with staff, pupils and parents.

Trinitas Academy Trust has a clear, progressive online safety education programme as part of the school's curriculum. This may include covering relevant issues through Relationships Education and Relationships and Sex Education (formerly known as Sex and Relationship Education), as well as DfE e-safeguarding, e-literacy framework, Personal, Social, Health and Economic (PSHE) education and other national guidance. Teachers will plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas. This covers a range of skills and behaviours appropriate to the child's age and experience.

**Teaching about online harms and risks in a safe way**
As with any safeguarding lessons or activities, it is important that the schools consider the topic they are covering and the potential that a child (or more than one child) in the class may be suffering from online abuse or harm in this way.
We will create a safe environment in which pupils feel comfortable to say what they feel.
In some cases, a pupil will want to make a disclosure following a lesson or activity. The lesson may have provided the knowledge that enabled the pupils to realise they are being abused or harmed and/or give them the confidence to say something. Schools will ensure that all pupils are clear what the schools reporting mechanisms are.
It will also include reflecting online behaviours in the school's behaviour and bullying policies.
Reference: PSHE Policy

**Prevent Awareness**
Pupils should be supported in building resilience to radicalisation. We will do this by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. (NB, Trinity Academy Trust adheres to all additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.)

It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be requested through the school's Every Compliance Management System, with clear reasons for the need.

### Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
The schools within the Trust runs a rolling programme of advice, guidance and training for parents/ carers in regards to online safety, including:

- Introduction of the Acceptable Use Policy to all parents, to ensure that principles of online behaviour are made clear;
- Information leaflets; in school newsletters; on the school website; letters home;
- Parent/carers awareness workshops held at school;
- Suggestions for safe Internet use at home.
- Links to relevant web sites / publications via the school's website
- Parents / Carers workshops
- Curriculum activities
- Safer Schools APP (Primary Schools)

## 5. Incident Management

- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that these will be dealt with quickly and sensitively, through the school's escalation processes.
- Monitoring and reporting of online safety incidents contribute to the development of policy and practice for online safety within the school.

- Support is actively sought from other agencies, as needed (e.g. the Local Authority and regional broadband grid, (London Grid for Learning LGFL) UK Safer Internet Centre helpline) in dealing with online safety issues.
- The records are reviewed/audited and reported to the school's senior leaders, and where appropriate Governors.
- Parents/carers are specifically informed of online safety incidents involving children for whom they are responsible.
- We will contact the Police if one of our staff, governors or pupils receives online communication that we consider is particularly disturbing or breaks the law.
- We will contact the Police if one of our staff, governors or pupils receives an email that we consider is particularly disturbing or breaks the law.

### Searching, Screening and Confiscation

The law allows school staff to search a pupil for any item if the pupil agrees. The Principal, Vice Principal or other authorised members of school staff have a statutory power to search pupils or their possessions, without consent, where they have reasonable grounds for suspecting that the pupil may have a prohibited item. Reference- Searching Screening and Confiscation Policy

### Data:

- Any data, files or images that **are believed** to be illegal must be passed to the police as soon as practicable, including pornographic images of children, without deleting them.

- Any data, files or images that **are not believed** to be unlawful, may be deleted or kept as evidence of a breach of the school's behaviour policy.

### Online (Cyber) Bulling

- Online/cyber bullying incidents are managed in line with our Behaviour Policy.
- Online bullying is unfortunately growing rapidly and some children have 24-hour access to the internet or a mobile phone and so it can be hard to escape.
- Some forms of online bullying can be:
  - **Peer-on-Peer abuse**
  - **Child Sexual Exploitation**
  - **Child on Child Sexual Violence and Harassment**
  - **Grooming**
  - **Radicalisation**
  - **Trolling**
- The audience for the bullying can be potentially huge and comments and pictures, including Youth Produced Sexual Imaging otherwise known as Sexting. (S*exting is when someone sends or receives a sexually explicit text, image or video on their mobile phone, usually in a text message and is likely to stay online forever).* **https://www.disrespectnobody.co.uk/sexting/what-is-sexting/**

### Child on Child Sexual Violence and Harassment

Sexual harassment is described as 'unwanted conduct of a sexual nature'. This applies to any form of online activity by a child that could be regarded as sexual harassment towards another child. Reference - Child on Child Sexual Violence and Harassment Between Children Policy

## 6. Handling complaints

The schools will take all reasonable precautions to ensure online safety. Trinitas Academy Trust and any of the schools within the Trust cannot accept liability for material accessed, or any consequences of internet access. Reference – Complaints Policy

Staff and pupils are given information about infringements in use and possible sanctions and may include:

**Pupils**

- Interview with the Principal;
- Informing parents or carers;
- If necessary referral to LA, CEOPs, Police.

**Staff**

Any complaint about staff misuse is referred to the Principal in the first instance for investigation and decision of action, which could include:

- Principal discussing the misuse with the Chief Executive Officer (CEO) and the Deputy Chief Executive Officer;
- Principal discussing the misuse with the Designated Safeguarding Lead;
- Principal informs the Chair and Safeguarding Governor of misuse;
- Reports to the Local Authority Designated Officer (LADO);
- Reporting to the Police

## 7. Equipment and Digital Content

### Mobile Technologies (including Bring Your Own Device BOYD) - staff

- Staff and visitors are permitted to use BOYD at Trinity School Belvedere in most areas of the school. The exception to this is;
- Mobile phones (except for mobiles provided by the school) and personally-owned devices will not be used in any way during lessons. They should be switched off or silent at all times and not visible to the pupils. This should also apply when children are attending after-school clubs or activities.
- Designated 'mobile use permitted' areas are situated in the primary schools, and signs to this effect are displayed.
- Personally owned IT equipment must not be connected to school wired networks.
- Personally owned equipment (including smart phones, tablets and laptops) may be registered for school Wi-Fi networks and used to access the Internet, but may not be joined to a domain or used to gain access to school internal network resources.
- Trinitas Academy Trust, and any of the schools within the Trust, accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school.
- The recording, taking and sharing of images of pupils is forbidden except for pre-authorised school purposes on school equipment.
- All content on school devices is subject to inspection.
- The school reserves the rights to search personal devices on school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.

### Mobile Technologies (including Bring Your Own Device BOYD) - pupils

*It is the discretion of the individual schools to allow pupils to have mobile phones.*

The primary schools have different age permissions for mobiles phones brought to school.

The following is expected of all primary pupils:

- Mobile phones must be turned off, not placed on silent, and handed to the designated member of staff (on arrival to school). Staff will hand back their mobile phones to the individual child at the end of the school day.
- If a pupil breaches the school policy, the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers only.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members.
- Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

**Years 7- 11**

- Pupils must not use their phones during the school day or have them out on display.

**Years 12-13**

- The phone can be used at any time except in lessons.

## 8. Emails

**Pupils:**

- Pupils use email as part of the IT/Computing scheme of work.
- Staff should not give personal (including personal work email address) to pupils or members of the Sixth Form.
- Pupils must not reveal private details of themselves.
- Pupils must immediately tell a teacher or responsible adult if they receive an e-mail which makes them feel uncomfortable, or is offensive or bullying in nature, and should not respond to malicious or threatening messages.
- Pupils must not arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them.
- Pupils must not delete malicious of threatening emails, but keep them as evidence of bullying.
- Pupils should not open attachments unless you are sure the source is safe.
- Forwarding 'chain' e-mail letters is not permitted.

**Staff:**

- Staff should not give their personal or work email to parents any communication should come through and be sent via the schools admin email address, unless there is a specific reason to not do so, e.g. school governors, Parent Teacher Association, Link Parent Forum, sharing of information. The emails must be sent in connection to the role and not for other purposes.
- Any information that includes personal data should be either anonymised and initials used only. If personal details need to be transmitted a secure process of online transfer such as Egress or LGFL's USO-FX must be used. Any other form of secure transmission must be approved by the Data Protection Officer prior to use.

## 9. School Website

- The Principals take overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- Photographs published on the website do not use pupils' full names in the text or in the file names or 'alt-tags' for images.

## 10. Social Networking

Teachers are instructed not to run social network spaces for pupils' use on a personal basis or to open up their own spaces to their pupils, but to use the schools' preferred system for such communications.

**School staff will ensure that in private use:**

- That they have a high level of privacy set. **BE AWARE THAT SOCIAL NETWORKING SITES UPDATE THEIR SECURITY SETTING, MEANING THAT PERSONAL SECURITY RIGHTS MAY BE JEOPARDISED.** It is your responsibility to ensure security settings are up to date and maintained.
- Remember that **ANYTHING YOU** post **CAN** and **DOES** end up in the public domain.
- Ex-pupils may be employed as staff – this can be particularly problematic, with 'friends' being both current colleagues and also former pupils and the user needs to consider this carefully when using social networking sites.
- No reference should be made in social media to pupils, parents/carers.
- **DO NOT** engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.

**Pupils are:**

- Advised to be very careful about placing any personal photos on any 'social' online network space.
- Taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Taught that they should not post images or videos of others without their permission.

## 11. Visitors

- Visitors (except supply teachers) are not permitted unsupervised access to any of the schools computing equipment.
- Visitors (including supply teachers) are not permitted to browse, download or send material that could be considered offensive if using a computer in school.
- All visitors must report any accidental access to, or receipt of inappropriate materials, or filtering breach to their sponsor.
- No visitor is permitted to download any software or resources from the internet that can compromise the network, or are not adequately licensed.
- No visitor is permitted to use personal digital cameras or camera phones for taking and transferring images of pupils or staff.

**Visitors' use of Bring Your Own Device (BOYD)**

- It is the discretion of the individual schools to allow visitors to use their electronic personal device including mobile phones whilst on the premises.

## 12. Review and Updates

- The Online Safety Policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the schools.

## Appendix 1: Staff AUP

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Principal and Governing Body.
- 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 email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business. (This is currently: LGfL)
- I will only use the approved school email, school Learning Platform or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work without the consent of the copywriter.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will ensure that I will only use my mobile phone in the designated areas of the school. I agree that under no circumstances should staff mobile phones be used or even visible in any other part of the school - this includes classrooms, corridors, halls, playgrounds including during break times and lunch times. (Primary schools only)
- I will use the school's Learning Platform in accordance with 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 agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.

- I will access school resources remotely (such as from home) only through the LGfL / school approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the 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 embed the school's online safety curriculum into my teaching.
- I will alert the school's named Designated Safeguarding Lead or child protection officer (CPO)/ relevant senior member of staff if I feel the behaviour of any child I teach may be a cause for concern.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that it is my duty to support a whole-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 a senior member of staff / named child protection officer at the school.
- I understand that failure to comply with this agreement could lead to disciplinary action.

**User Signature**

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety policies.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature ............................................Date .........................................

Full Name ........................................................................... (printed)

Job title .............................................................................................................

School ...............................................................................................................

**Authorised Signature (Principal)**

I approve this user to be set-up.

Signature…………………………………………… Date………………………

Full Name…………………………………………… (printed)

*Appendix 2: Pupil AUP EYFS and KS1*

# *Think before you click*

**EYFS and KS1 Acceptable Usage Policy**

| | |
|---|---|
| S | I will only use the Internet and email with an adult. |
| A | I will only click on icons and links when I know they are safe. |
| F | I will only send friendly and polite messages. |
| E | If I see something I don't like on a screen, I will always tell an adult. |

Print Child's Name:

Parent's Signature:

Date:

## *Appendix 3: AUP for KS2 Pupils*

*These rules will keep me safe and help me to be fair to others.*

- I will only use the school's computers and tablets for schoolwork and home learning.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that 'social network sites should never be accessed/used within school'.
- I will not attempt to visit internet sites that I know to be banned by the school.
- I will only email people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.
- If given permission to have a mobile phone in school I will not use it whilst on the school premises to communicate, take photos/videos or be part of a social networking group e.g. WhatsApp or Facebook.

*I have read and understand these rules and agree to them.*

Print child's name:

Child's Signature: Date:

*Appendix 4: AUP for KS3 & 4*

# TRINITY SCHOOL, BELVEDERE

## Using the Internet and school network

### TO PARENTS AND GUARDIANS

The school provides supervised internet access to support learning and to equip pupils with life skills, including developing the skills and awareness to use public domain resources safely and responsibly. We believe that internet access at home can also be of great benefit to pupils, but parents are warned that some on-line materials are potentially harmful, and that adult supervision is advisable.

For more information on internet safety, visit the Child Exploitation & Online Protection Centre website at www.ceop.gov.uk.

### TO PUPILS

When using school ICT resources:-

- I will respect the Trinity Code.
- I will take good care of equipment and passwords.
- I will use them positively and appropriately.

The school may restrict computer use because of privacy, copyright and licence conditions, personal safety and the need to share limited resources fairly. I understand that the following are not allowed on school computers:-

- Using chat rooms, instant messaging and social networking.
- Using irrelevant or inappropriate sites in lesson time.
- Any use apart from coursework or homework at lunchtime.
- Streaming audio or video, including internet radio, except under a teacher's direct supervision, as this slows down the network.
- Visiting any web site that breaks the Trinity Code, or allows access to content blocked by school policy or filtering, or wastes school resources.
- Making purchases or giving out personal information via the internet.

The school monitors use of its computer systems and may check or delete any file. If anyone breaks the above agreement, the full range of school sanctions may be applied.

Signed: ________________________________________

*Appendix 5: AUP for KS5*

# TRINITY SCHOOL, BELVEDERE

## Using the Internet and school network

### TO PARENTS AND GUARDIANS

The school provides supervised internet access to support learning and to equip students with life skills, including developing the skills and awareness to use public domain resources safely and responsibly. We believe that internet access at home can also be of great benefit to students, but parents are warned that some on-line materials are potentially harmful, and that adult supervision is advisable.

For more information on internet safety, visit the Child Exploitation & Online Protection Centre website at www.ceop.gov.uk.

### TO STUDENTS

When using school ICT resources:-

- I will respect the Trinity Code.
- I will take good care of equipment and passwords.
- I will use them positively and appropriately.

The school may restrict computer use because of privacy, copyright and licence conditions, personal safety and the need to share limited resources fairly. I understand that the following are not allowed on school computers:-

- Using chat rooms, instant messaging and social networking.
- Using irrelevant or inappropriate sites in lesson time.
- Any use apart from coursework or homework at lunchtime or in study periods.
- Streaming audio or video, including internet radio, except under a teacher's direct supervision, as this slows down the network.
- Visiting any web site that breaks the Trinity Code, or allows access to content blocked by school policy or filtering, or wastes school resources.
- Making purchases or giving out personal information via the internet.

The school monitors use of its computer systems and may check or delete any file. If anyone breaks the above agreement, the full range of school sanctions may be applied.

Signed: _______________________________________

***Appendix 6: Parent AUP***

## *Trinitas Academy Trust*

## Online Safety Acceptable Usage Policy: Parents

**Internet and ICT:** As the parent or legal guardian of the pupil(s) named below. Please be aware that your *daughter / son* will have access to:

- the Internet at school
- the school's chosen email system
- ICT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's online safety or e-behaviour they will contact me and reserve the right to delete any files.

I understand that the school will use, when necessary, photographs of my child or include them in video material to support learning activities.

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose, for example, the school's website.

I will not take photographs or videos of other children (or staff) at school events.

**Social networking and media sites:** I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I will support the school by promoting safe use of the Internet and digital technology at home.  I will consult the school if I have any concerns.

**Child's name: _______________________________________**

**Parent / guardian signature:** ______________________________

**Date: ___/___/___**

*Appendix 6: Parent AUP*

## The Use of Social Networking and Online Media

This school asks its whole community to promote the three common approaches to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

*How do I show common courtesy online?*

- I do not upload photographs, videos or any other information about someone or groups of people online without their permission.
- I do not post hurtful, rude or derogatory comments or materials. To do so is disrespectful and may upset, distress, bully or harass.

*How do I show common decency online?*

- I do not post **intimidating, racist, sexist, homophobic or defamatory comments. This is online bullying** and may be harassment or libel.
- When such comments exist online, I do not forward them. By creating or forwarding such materials I am liable under the law.

*How do I show common sense online?*

- I think before I click.
- I think before I upload comments, photographs and videos.
- I think before I download or forward any materials.
- I think carefully about what information I share with others online, and I check where it is saved and check our privacy settings and take note of any changes made by the social networking service provider.
- I block harassing communications and report any abuse.

**The school will respond to any actions online that bring the school into disrepute.**

In the event that any pupil or parent/carer is found to be posting libellous or inflammatory comments on Facebook, Twitter or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.
*(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)*
Pupils may be subject to school disciplinary actions. Parents may be subject to civil or legal criminal proceedings.

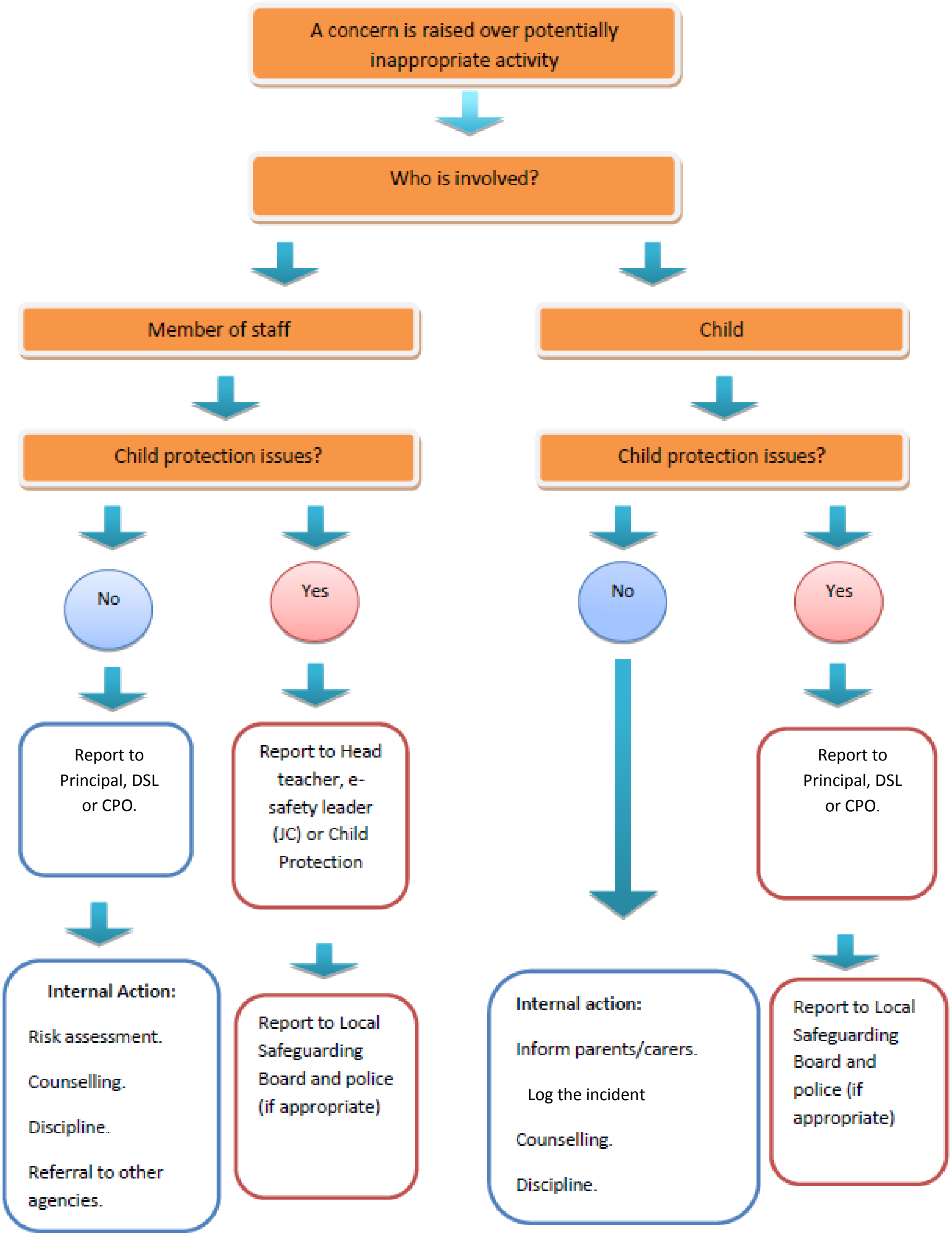
In serious cases the school will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process:
https://www.thinkuknow.co.uk/parents/browser-safety/

## *Appendix 7: Protocol for responding to online safety incidents*

**Policy: How will infringements be handled**?

Whenever a pupil or staff member infringes the online safety Policy, the final decision on the level of sanction will be at the discretion of the school management and will reflect the school's behaviour and disciplinary procedures.


A concern is raised over potentially inappropriate activity
Who is involved?
Member of staff
Child
Child protection issues?
Child protection issues?
No
Yes
No
Yes
Report to Principal, DSL or CPO.
Report to Head teacher, e-safety leader (JC) or Child Protection
Report to Principal, DSL or CPO.
Internal Action:
Risk assessment.
Counselling.
Discipline.
Referral to other agencies.
Report to Local Safeguarding Board and police (if appropriate)
Internal action:
Inform parents/carers.
Log the incident
Counselling.
Discipline.
Report to Local Safeguarding Board and police (if appropriate)

## Appendix 8: Reference

- Keeping Children Safe in Education (September 2019)
  **https://www.gov.uk/government/publications/keeping-children-safe-in-education--2**

- UK Council for Child Internet Safety (UKCCIS) Guidance (January 2017)
  https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

- Searching, Screening and Confiscation guidance (January 2018)
  https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674416/Searching_screening_and_confiscation.pdf

- Sexual violence and sexual harassment between children in schools and colleges (May 2018)
  https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/719902/Sexual_violence_and_sexual_harassment_between_children_in_schools_and_colleges.pdf

- Relationship Education, Relationships and Sex Education and Health Education
  https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education

## Appendix 9: Links to other organisations or documents

NSPCC https://www.nspcc.org.uk/
Safer Internet Centre – http://saferinternet.org.uk/
South West Grid for Learning - http://swgfl.org.uk/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk/

**CEOP**

CEOP - http://ceop.police.uk/ Online safety education programme from the National Crime Agency's CEOP Command which aims to safeguard children from sexual abuse and exploitation. Education resources and online advice for children aged 4 – 18. https://www.thinkuknow.co.uk/
INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis

**Bullying / Cyberbullying**

DfE - Cyberbullying guidance -
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – new Cyberbullying guidance and toolkit (Launch spring / summer 2016) -
http://www.childnet.com/new-for-schools/cyberbullying-events/childnets-upcoming-cyberbullying-work
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

**Social Networking**

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people

Connectsafely Parents Guide to Facebook

Facebook Guide for Educators

**Curriculum**

SWGfL Digital Literacy & Citizenship curriculum

**Data Protection**

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Guide to the Freedom of Information Act - https://www.gov.uk/make-a-freedom-of-information-request

**Working with parents and carers**

SWGfL Digital Literacy & Citizenship curriculum

Online Safety BOOST Presentations - parent's presentation

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Teach Today - resources for parents workshops / education

Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide

Insafe - A guide for parents - education and the new media

## Appendix: 10: Glossary of Terms

| | |
|---|---|
| **AUP** | Acceptable Use Policy – see templates earlier in this document |
| **CEOP** | Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes. |
| **BOYD** | Bring Your Own Device |
| **CPO** | Child Protection Officer |
| **DFE** | Department of Education |
| **DSL** | Designated Safeguarding Lead |
| **EYFS** | Early Years Foundation Stage |
| **LADO** | Local Authority Designated Officer |
| **IT** | Information and Technology |
| **IP address** | The label that identifies each computer to other computers using the IP (internet protocol) |

| | |
|---|---|
| **ISP** | Internet Service Provider |
| **IWF** | Internet Watch Foundation |
| **LA** | Local Authority |
| **PSHE** | Personal Social Health Education |
| **SIMs** | Information Management System |
| **SIRO** | Senior Information Risk Officer |
| **SWGfL** | South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW |
| **TUK** | Think U Know – educational e-safety programmes for schools, young people and parents. |
| **UKSIC** | UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation. |