

ICT and Online Safety Policy

Category:	Trust-wide Policy
Authorised By:	Board of Trustees
Author:	Sumit Parmar, <i>ICT Manager</i> Catherine Roper, <i>Marketing & Communications Manager</i>
Owner:	Sudhi Pathak; Chief Operating Officer
Version:	7
Status:	Ratified
Issue Date:	March 2026
Next Review Date:	March 2027

Version Control

<u>Ver.</u>	<u>Date</u>	<u>Comment</u>
1	June 2018	
2	January 2021	Cyclical review. Updated against Schools HR model and incorporating the Social Media Policy
3	April 2022	Cyclical review
4	April 2023	Cyclical review
5	March 2024	Cyclical review; no changes
6	March 2025	Cyclical review. Updates to the Social Media Policy
7	March 2026	Cyclical review. No substantive changes

This policy will be subject to ongoing review and may be amended prior to the scheduled date of the next review in order to reflect changes in legislation, statutory guidance, or best practice (where appropriate).

Contents

1. Introduction	5
2. Aims	5
3. Legislation and guidance	5
4. Monitoring and review	6
5. Scope of the policy	6
6. Roles and responsibilities	7
6.1. The Board of Trustees	7
6.2. Heads and Senior Leaders	7
6.3. Designated Safeguarding Lead (DSL)	8
6.4. ICT Manager	8
6.5. All staff and volunteers	9
6.6. Parents and carers	10
6.7. Pupils	10
6.8. Visitors and community users	11
7. Social media policy	11
7.1. Introduction	11
7.2. Scope	12
7.3. Using social media on behalf of the Trust	12
7.4. Raising concerns	16
7.5. Disciplinary action	16
7.6. Monitoring	16
8. Other policy statements	16
8.1. Education: Pupils	16
8.2. Education: Parents and carers	17
8.3. Education & Training: Staff and volunteers	17
8.4. Technical: Infrastructure, equipment, filtering and monitoring	17
9. Mobile technologies	19
9.1. Personal devices:	20
10. Staff using work devices outside school	20
11. Use of digital and video images	20
12. Data protection	21
13. Communications	23
14. Unsuitable and/or inappropriate activities	24
15. Responding to incidents of misuse	26
15.1. Illegal incidents	26

15.2. Other incidents	27
16. Eden Academy Trust actions & sanctions	28
16.1. Pupil incidents	29
16.2. Staff incidents	31
17. Links with other policies	32
Appendix 1: Acceptable use agreement – Staff, Members, Trustees, LAB/Committee members, volunteers, and visitors	33
Appendix 2: Acceptable use agreement – pupils and parents/carers	34

1. Introduction

This IT and Online Safety Policy (this Policy) has been updated from an initial version which had been developed by a working group made up of the then Director of Academy Development, an Academy Associate Head and a representative of the Board of Trustees and was reviewed by:

- Heads¹
- Staff – including Teachers, Therapy staff and Support Staff,
- The Eden Academy Trust's (the Trust) technical support provider
- Local Advisory Boards
- Parents and Carers

Subsequent updates have been reviewed by the ICT Manager, Marketing & Communications Manager, IT Strategy Group, Heads, the Trustee portfolio holder and/or the Senior HR Adviser as appropriate.

2. Aims

The Trust aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

3. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on [preventing and tackling bullying](#) and [searching, screening and confiscation](#). It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

¹ For the purposes of this Policy, Head refers to Headteacher or Head of School as appropriate

This policy complies with our funding agreement and Articles of Association.

4. Monitoring and review

Implementation of this policy will be undertaken by the Trustee portfolio holder for ICT who will receive a termly report on its implementation generated by the ICT Manager, which will include anonymous details of online safety incidents. The portfolio holder will report back to the Board as appropriate.

Should serious online safety incidents take place, the following external persons and/or agencies should be informed:

- The school's DSL and the Trust's safeguarding lead
- Trustee portfolio holder (in the termly report)
- ICT Manager
- And in exceptional cases to the LADO and the Police

The Trust and its internet service providers will monitor the impact of the policy using:

- Logs of reported incidents from schools
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity

5. Scope of the policy

This policy applies to all members of the Eden Academy Trust Community (including Trustees, staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Trust's ICT systems², both in and outside the Trust.

This version incorporates the Trust's Social Media Policy which is based on the model policy from the Schools HR Co-operative. This applies to all employees whether in one of the Trust's schools, setting or the central team. It also applies to all Members, Trustees and LAB/Committee members across the Trust.

The Education and Inspections Act 2006 empowers Heads³ to such extent as is reasonable, to regulate the behaviour of pupils when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion

² For the purposes of this Policy, all references to the Trust's equipment, infrastructure, systems etc. refers also to the same at any of the Trust's schools.

³ For the purposes of this policy, Head refers to Executive Head, Headteacher or Head of School/Setting/Satellite as appropriate

of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

6. Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the Eden Academy Trust. (the Trust).

6.1. The Board of Trustees

The Board of Trustees (the Board) has overall responsibility for monitoring this policy and holding the Executive Team (and through them the Heads) to account for its implementation. The Board will review effectiveness by receiving regular information about online safety incidents and monitoring reports from the Trustee ICT portfolio holder. The Board's safeguarding Trustee portfolio holder will also receive appropriate information regarding any safeguarding incidents through the safeguarding hub and the Trust's safeguarding lead.

All Trustees, along with Members and Local Advisory Board/independent committee members will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

The Board will ensure that appropriate filtering and monitoring systems are in place, whilst being careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

6.2. Heads and Senior Leaders

- The Head has a duty of care for ensuring the safety, including online safety, of members of the school community, though the day to day responsibility for online safety will be delegated member of staff.
- The Head and (at least) another member of the School Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. See the Dealing with Allegations of Abuse against staff guidelines.
- The Head is responsible for ensuring that the online safety teacher and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. See Online Safety guidelines for staff, parents and carers.
- The Head will enable a system in their school/setting/satellite to allow for monitoring and support of those in school who carry out the internal online

safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. Support will be provided by the external ICT support provider.

- The Regional Director with responsibility for safeguarding and child protection will receive regular reports on matters of online safety from Heads.
- Similar responsibilities will apply to the CEO, Deputy CEO and COO in relation to centrally contracted staff.

6.3. Designated Safeguarding Lead (DSL)

Details of the Trust's designated safeguarding leads and deputies are set out in our [child protection and safeguarding policy](#).

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Head in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Head, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Head.

This list is not intended to be exhaustive.

6.4. ICT Manager

The Trust's ICT Manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the Trust's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the Trust's ICT systems on a weekly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

6.5. All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of online safety matters and of this policy and have read, understood and signed the Acceptable Use Agreement (appendix 1).
- Implementing this policy consistently.
- Ensuring that pupils understand and follow the Trust's IT & Online Safety Policy guidelines as appropriate.
- Reporting any suspected misuse or problem to the Head or ICT Manager for investigation/action/sanction.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the relevant school's behaviour policy.
- Ensuring that all digital communications, particularly with pupils and/or parents/carers are on a professional level and be made using Eden email addresses. Staff should **not** use personal email addresses for official communications.- See the Trust's [Child Protection and Safeguarding Policy and Guidance for Safer Working Practice](#).
- Ensuring that online safety issues are embedded in all aspects of the curriculum and other activities.
- Ensuring that the whole school community has a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Monitoring the use of digital technologies, mobile devices, cameras and similar devices in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- Ensuring that whenever the internet is used, pupils are guided to sites suitable for their use and that processes are in place for dealing with any unsuitable material from internet searches.

This list is not intended to be exhaustive.

6.6. Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet along with mobile and similar devices in an appropriate way. The Trust will take every opportunity to help parents and carers understand these issues through parents' evenings, newsletters, letters, website and information about national and local - safety campaigns or literature. Parents and carers will be encouraged to support the Trust in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Access to parents' sections of the website, learning platforms and online pupil records.
- Their children's personal devices in the school, where this is allowed.

Parents are expected to:

- Notify a member of staff or the Head of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the Trust's ICT systems.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? UK Safer Internet Centre:
<https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>
- Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>
- Parent factsheet, Childnet International:
<http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf>

6.7. Pupils

Pupils will be expected and supported to:

- Use the Trust's digital technology systems in accordance with the Pupil Acceptable Use Agreement (appendix 2) which they should sign; where appropriate it would be expected that parents or carers would sign on behalf of the pupils.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

- Will be expected to know and understand policies on the use of mobile devices, digital cameras and similar devices. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Trust's IT & Online Safety Policy covers their actions out of school, if related to their membership of the school.
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology.

6.8. Visitors and community users

Visitors and members of the community who use the Trust's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

7. Social media policy

7.1. Introduction

For the purposes of this policy, *Social Media* is any type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes but is not limited to online social forums such as X (formerly Twitter), Facebook, WhatsApp, Instagram, LinkedIn and BlueSky. Social media also covers blogs and video and image sharing websites such as YouTube, TikTok, Vimeo and Flickr.

Whilst recognising the benefits of social media and the opportunities for communication this provides, this Policy sets out the principles which staff, volunteers and contractors are expected to follow when using social media to ensure the Trust upholds the highest possible standards of confidentiality and accountability and to ensure that its reputation and that of its pupils is safeguarded at all times.

All staff working within the school are in a position of trust, they are therefore required to familiarise themselves with this Policy and raise any concerns where they may arise to safeguard our children and protect our staff.

Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites; Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be embarrassing if too much personal information is known in the work place. Staff should not "befriend" pupils, parents or carers on social media.

Staff should be aware that there are many more examples of social media than can be listed here and this is a constantly changing area.

Staff should follow these guidelines in relation to any social media that they use both in work and in their private lives.

7.2. Scope

The Social Media Policy outlined in this section, applies to employees who are directly employed by the Trust, either in its schools or the central team. It also applies to all volunteers, contractors, Members, Trustees and LAB/Committee members across the Trust.

The aim is to advise staff and others of the expectation of working in a school environment when using social media, and highlighting:

- The importance of ensuring that relevant privacy settings are activated and regularly reviewed.
- The restrictions of maintaining a professional relationship and professional conduct are adhered to.
- Guidance on what is acceptable and what is unacceptable when using social media.

To identify responsibilities of the school and its staff in line with the relevant policies including:

- ICT Usage
- Anti-Bullying & Harassment
- Code of Conduct

7.3. Using social media on behalf of the Trust

The Trust expects all staff (including the governance community and other volunteers) to consider the safety of pupils and the risks (reputational and financial) to the school when using social media channels, including when doing so in a personal capacity. Staff are also responsible for checking and maintaining appropriate privacy and security settings of their personal social media accounts.

Staff members will report any safeguarding issues they become aware of.

Only official school sites must be used for communicating with pupils or to enable pupils to communicate with one another. There must be a strong pedagogical or business reason for creating official school sites to communicate with pupils or others, and written consent from the Head must be obtained. Sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements. Staff must not create sites for trivial reasons which could expose the school to unwelcome publicity or cause reputational damage.

Staff are not allowed to access social media websites from the Trust's computers or devices at any time unless written consent has been obtained from the Head. This includes any portable devices e.g., tablets, smartphones etc. provided by the school for work purposes. As such, each school will have filters in place to restrict social media access as appropriate. Staff should not access social media for personal use on Trust devices unless written consent has been obtained from the Head or the service manager.

Any recording devices e.g., cameras, video cameras, mobile phones etc. must only be used for specified purposes as directed by the school.

Please note: while we recommend members of staff make their private social media profiles unidentifiable to pupils, we understand many staff will use sites such as X (formerly Twitter) or LinkedIn for professional purposes.

When using social media, staff must not:

- Use personal accounts to conduct school business
- Accept 'friend requests' from, or communicate with, pupils or their families past or present
- Complain about the school, individual pupils, colleagues or parents/carers
- Reference or share information about individual pupils, colleagues or parents/carers
- Post images of pupils
- Express personal views or opinions that could be interpreted as those of the school
- Make any comment on social media that has the potential to bring the Trust into disrepute. This will include remarks or comments which may be perceived to negatively reflect on others with protected characteristics.
- Link their social media profile to their work email account*
- Use personal social media during timetabled teaching time except in a professional capacity [delete as appropriate]
- Any concerns regarding a member of staff's personal use of social media will be dealt with in line with the staff behaviour policy.

13

Any communication received from current pupils (unless they are family members) on any personal social media accounts will be reported to the designated safeguarding lead (DSL) or member of the senior leadership team immediately.

Staff should not also do not have contact via personal accounts with past pupils or their families (if ongoing communication is required, this should be using via official school channels).

*Staff may reference their employer in such cases but all communication on the site should meet the social media guidelines.

The Trust understands that staff may wish to use their own computers or devices, such as laptops, smartphones and/or smart watches, to access social media websites whilst they are at work. Staff must limit their use of social media on their own equipment to their official rest breaks such as their lunch breaks. Devices such as smart watches come under the same usage in school as mobile phones and should not be used when you are in the classroom.

Staff using social media in a personal capacity outside of the school environment must recognise that whilst they are not acting on behalf of the school/Trust, the school/Trust may be adversely affected if the school/Trust is identified as the staff members' place of work and negative or inappropriate comments are made. Staff are permitted to say that they work for the school, which recognises that it is natural for its staff to sometimes want to discuss their work on social media. However, the staff member's online profile name must not contain the school/Trust's name.

Staff must also be mindful of the information they put on social media and consider how this will reflect on the school, its staff, pupils and their families:

- **It should not bring the organisation into disrepute, for example by:**
 - Maintaining any relationship with pupils on social media e.g. staff should decline 'Friend' requests, unless the pupil(s) are immediate family members. If requests are received from pupils who are not family members, this must be raised with the Headteacher or another member of the Senior Management Team. Measures will then be taken to communicate to students that such connections should be with the School's official site where appropriate;
 - Having any contact with pupils' family members through social media if that contact is likely to constitute a conflict of interest or call into question their objectivity;
 - Criticising or arguing with parents, colleagues etc;
 - Making defamatory comments about individuals or other organisations or groups;
 - Posting images that are inappropriate or links to inappropriate content;
 - Giving personal contact details to children or young people, including their mobile telephone number or personal email address;
 - Using personal equipment (e.g., mobile phone device) to communicate with children or young people;
 - Not having the relevant written permission from parents for communication, using the school's equipment, permission must detail the specific reasons why this communication is required;
 - Making contact for personal reasons;
 - Using the internet or other communication channels to send personal messages to children/young persons;
 - Responding to/ request personal information from a child or young person, other than that which might be appropriate as part of your professional role;

- Mentioning in a negative manner, the school its pupils, parents or colleagues;
- Commenting on any incidents that occur or have occurred within the school;
- Posting photographs, videos or any other types of image of pupils and their families.
- **Breach confidentiality, for example by:**
 - Discussing confidential or personal information about an individual (such as a colleague or pupil) or organisation (such as a supplier of services);
 - Discussing the school's internal workings (such as ongoing Personnel issues, or its future business plans that have not been communicated to the wider public);
 - The school does not expect staff members to discontinue contact with their family members via personal social media once the school starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way;
 - School email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.
- **Do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:**
 - Making offensive or derogatory comments relating to age, disability, gender reassignment, race (including nationality), religion or belief, sex and sexual orientation;
 - Using social media to bully another individual (such as a staff member of the school); or
 - Posting images that are or are likely to be considered discriminatory or offensive;
 - Using social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations.
- **Breach copyright, for example by:**
 - Using someone else's images or written content without permission;
 - Failing to give acknowledgement where permission has been given to reproduce something.

- **Other**

- No contact should be made via social media with pupils unless they are immediate family members.

7.4. Raising concerns

Any concerns should be raised with your Line Manager or school Head.

7.5. Disciplinary action

All staff within the school are required to adhere to this policy.

Staff should note that any breaches of this policy may lead to disciplinary action. Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing serious damage to the school or Trust, may constitute gross misconduct and lead to summary dismissal.

Where a contractor becomes aware that one of their employees has breached this policy they will need to notify the Trust, and ensure that appropriate action is taken against the employee.

7.6. Monitoring

All school ICT systems may be monitored in accordance with the School's ICT Usage Policy, so personal privacy cannot be assumed when using school hardware.

Schools can monitor the usage of its own internet and email services without prior notification or authorisation from users (staff, contractors and pupils) when justifiable concerns have been raised re: electronic communication.

16

8. Other policy statements

8.1. Education: Pupils

The policy statement relevant to students and pupils are contained in the Trust User Guidelines.

Pupils will be taught about online safety as part of the curriculum as appropriate to their age and ability.

This will include:

- Using technology safely, respectfully and responsibly, keeping personal information private and protecting their online identity and privacy.
- Identify where to go for help and support when they have concerns about content, contact or conduct on the internet or other online technologies and know how to report concerns.
- Recognise acceptable and unacceptable behaviour, inappropriate content, contact and conduct.

The safe use of social media and the internet will also be covered in other subjects where relevant. The school will use assemblies to raise pupils' awareness of the

dangers that can be encountered online and may also invite speakers to talk to pupils about this.

8.2. Education: Parents and carers

Many parents and carers may 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 and regulation of the children's on-line 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 Trust will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, virtual learning environments
- Parents/carers sessions
- High profile events and campaigns, e.g. Safer Internet Day
- Reference to the relevant web sites and publications

This policy will also be shared with parents. Concerns or queries about this policy can be raised with any member of staff or the Head.

8.3. Education & Training: Staff and volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training annually and as part of induction will be made available to staff. Schools will keep records of the training delivered.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand this policy along with the ICT Usage Policy and the accompanying Acceptable Use Agreement.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- This policy will be presented to and discussed by staff.

8.4. Technical: Infrastructure, equipment, filtering and monitoring

The Trust will be responsible for ensuring that the Trust infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people identified in the above sections will be effective in carrying out their online safety responsibilities:

- Technical systems will be managed in ways that ensure that the Trust meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of Trust technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to academy technical systems and devices.
- Users (where appropriate) will be provided with a username and secure password by the Head, line manager or ICT Manager.
- Users are responsible for the security of their username and password and will be expected to change their password(s) periodically in line with Trust procedures. Staff must not share passwords or allow anyone else access to their network account and must not give their family members access to Trust's ICT facilities (devices, systems or accounts).
- The "master and administrator" passwords for the Trust's ICT systems, used by the ICT Manager (or other person) must also be available to the Head and kept in a secure place.
- The Trust's ICT Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband provided by The London Grid for Learning by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored. Requests for filtering changes must be made through the Head or ICT Manager.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The Trust has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff, pupils/students). Requests for filtering changes must be made by the Head or Cabinet member.
- The Trust's ICT provider regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual or potential technical incident or security breach to the relevant person, as agreed.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobiles, tablets or similar devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The Trust's infrastructure and individual workstations are protected by up-to-date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff, pupils, community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g., memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. External drives/CD/DVD to not be used on the school network unless authorised by either the Head or ICT Manager. When personal data is stored on any portable computer system, memory stick or any other removable media:
 - The data must be encrypted, and password protected.
 - The device must be password protected.
 - The device must offer approved virus and malware checking software.
 - The data must be securely deleted from the device, in line with Trust policy (below) once it has been transferred or its use is complete.

9. Mobile technologies

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, notebook, laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use mobile and personal devices in a school context is educational. The schools' mobile technologies policies should be consistent with and inter-related to other relevant school and Trust policies including, but not limited to the Child Protection and Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe

and appropriate use of mobile technologies should be an integral part of the Trust's online safety education programme.

- The Trust's Acceptable Use Agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies.
- The Trust allows the use of personal devices for school business (email, Schoolwork) but not for the storage of images.

9.1. Personal devices

- Users are allowed to use personal mobile devices in break times and for school business (staff, pupils, students and/or visitors).
- Taking, storage and/or use of images is not permitted on personal devices.
- The Trust's policy regarding the use of mobile devices is included in the Staff Acceptable Use Agreement.
- Personal devices will be kept out of sight of children and not used in classrooms.
- The Trust is not liable for loss, damage or malfunction following access to the network.
- Technical support will not be available for personal devices.
- The Trust has the right to take, examine and search user devices in the case of misuse following the recommended legal guidelines.

20

10. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

11. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. As well as any inherent safeguarding issues, such images may provide avenues for cyber-bullying to take place. Digital images may remain

available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images.
- In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, social media and/or local press.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at Trust events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow Trust policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Trust equipment; the personal equipment of staff must not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school/Trust into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the student/pupil and parents or carers.

12. Data protection

Please Note: The Data Protection Act has been replaced by the General Data Protection Regulations which came into force on 25th May 2018. The Trust has

scrutinised the new regulations to ensure that the latest requirements are incorporated in this IT & Online Safety Policy

Currently, personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Only transferred to others with adequate protection.

The Trust must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy.
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA).
- Risk assessments are carried out.
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.

- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media

- All external personal devices, which include memory sticks or any other removable media, are not permitted on the school's network unless authorised by the Head or the ICT Manager.
- When permission has been granted the data must be encrypted, and password protected.
- The data must be securely deleted from the device, in line with Trust policy (below) once it has been transferred or its use is complete.

13. Communications

23

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following shows how the Trust currently considers the benefit of using these technologies for education outweighs their risks and/or disadvantages.

When using communication technologies Eden Academy Trust considers the following as good practice:

- **The official Trust email service may be regarded as safe and secure and is monitored.** Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school/Trust email service to communicate with others when in school, or on school/academy systems (e.g., by remote access).
- **Users must immediately report to the nominated person – in accordance with the Trust policy - the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official

(monitored) school/Trust systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Whole class/group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school/Trust email addresses for educational use, as appropriate to meet the varying needs of our children in different situations
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school or Trust website and only official email addresses should be used to identify members of staff.
- All work related communications between staff are considered to be professional communications. As such these work related exchanges on personal devices or Eden devices are subject to the same standards as set out in this document.

14. Unsuitable and/or inappropriate activities

Some internet activity e.g., accessing child abuse images or distributing racist material is illegal and is obviously banned from academy and all other technical systems. Other activities e.g., cyber-bullying is inappropriate behaviour and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in the academy context, either because of the age of the users or the nature of those activities.

The Trust believes that the activities referred to in the following section would be inappropriate in the academy context and that users, as defined below, should not engage in these activities either in or outside the Trust when using Trust equipment or systems. The Trust policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download,	Child sexual abuse images – the making, production or distribution of indecent images of children - contrary to The Protection of Children Act 1978					✓
	Grooming, incitement, arrangement or facilitation of sexual acts against children contrary to the Sexual Offences Act 2003.					✓

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) contrary to the Criminal Justice and Immigration Act 2008					✓
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) contrary to the Criminal Justice and Immigration Act 2008					✓
	Pornography				✓	
	Promotion of any kind of discrimination					✓
	Threatening behaviour, including promotion of physical violence or mental harm					✓
	Promotion of extremism or terrorism					✓
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the Trust/school into disrepute				✓	
Using school systems to run a private business						✓
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/Trust					✓	
Infringing copyright						✓
Revealing or publicising confidential or proprietary information (e.g. financial and/or personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files						✓
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					✓	
Online gaming (educational)			✓			
Online gaming (non-educational)					✓	
Online gambling					✓	
Online shopping/commerce			✓			
File sharing				✓		
Use of social media				✓		

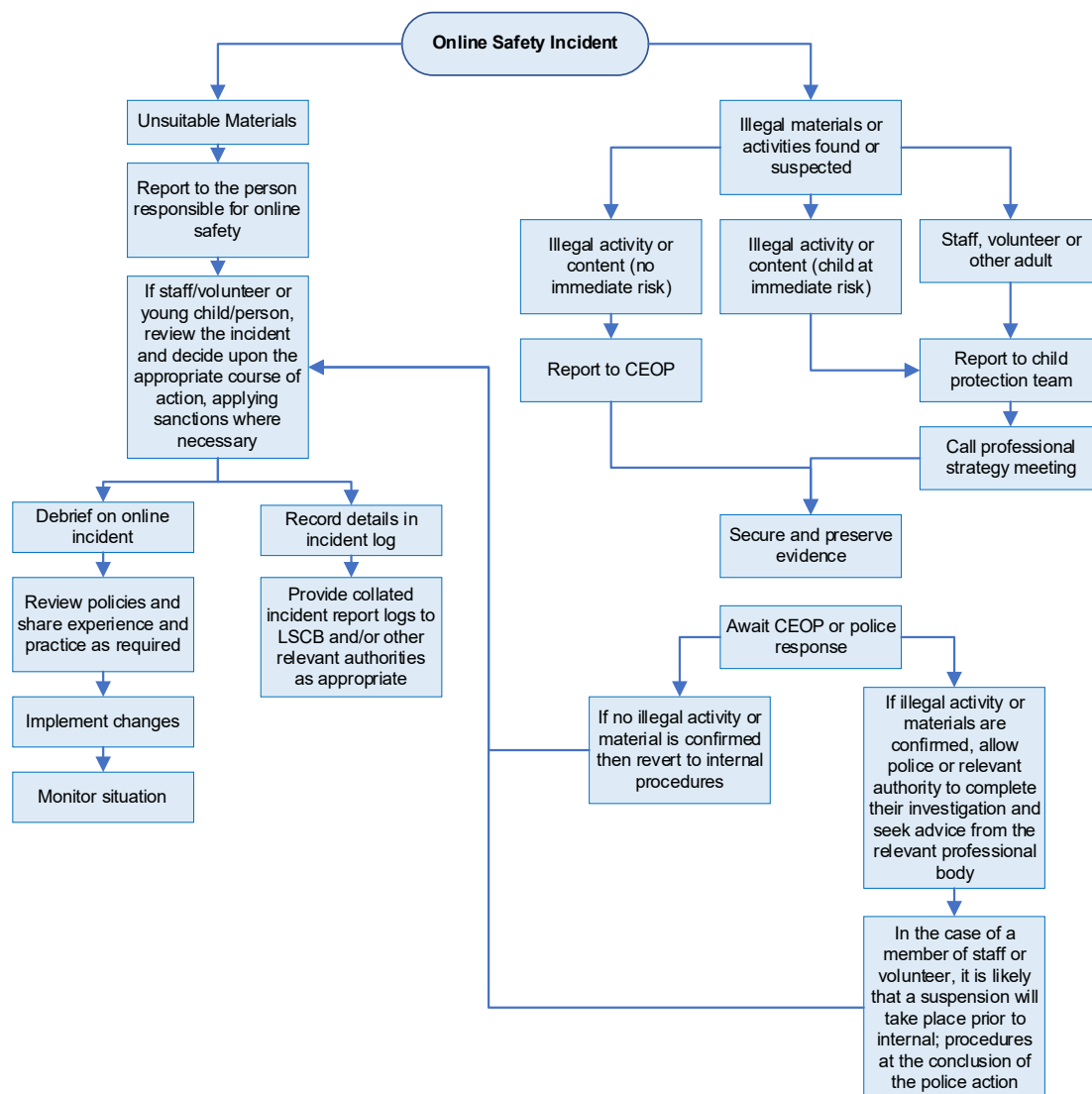
User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Use of messaging apps			✓		
Use of video broadcasting e.g. YouTube			✓		

15. Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

15.1. Illegal incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



15.2. Other incidents

It is hoped that all members of the Trust community will be responsible users of digital technologies, who understand and follow academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff or local Advisor involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure. Involve the technical service provider where appropriate.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by the Academy Group
 - Police involvement and/or action
- **If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - promotion of terrorism or extremism
 - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the Trust and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

16. Eden Academy Trust actions & sanctions

It is more likely that the Trust will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

As well as the Actions and sanctions for student incidents identified below, each school will have agreed sanctions depending on the behaviour identified.

As well as the actions and sanctions for Staff incidents identified below, schools will need to follow the Academy Disciplinary Policy.

The Trust or schools within the Trust will take advice for the Local Authority Designated Officer for Safeguarding.

16.1. Pupil incidents

Pupil incidents	Refer to class teacher	Refer to Head of Department / Year / other	Refer to Head	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓		✓			
Unauthorised use of non-educational sites during lessons			✓			✓			
Unauthorised / inappropriate use of mobile phone, digital camera and/or other mobile devices			✓			✓			
Unauthorised / inappropriate use of social media, messaging apps and/or personal email			✓			✓			
Unauthorised downloading or uploading of files			✓			✓			
Allowing others to access school / Trust network by sharing username and passwords			✓			✓			
Attempting to access or accessing the school / Trust network using another pupil's account			✓			✓			
Attempting to access or accessing the school / Trust network using the account of a member of staff			✓			✓			
Corrupting or destroying the data of other users			✓			✓			

Pupil incidents	Refer to class teacher	Refer to Head of Department / Year / other	Refer to Head	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			✓			✓			
Continued infringements of the above, following previous warnings or sanctions			✓	✓		✓			
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the school / Trust			✓			✓			
Using proxy sites or other means to subvert the school / Trust's filtering system			✓		✓	✓			
Accidentally accessing offensive or pornographic material and failing to report the incident			✓		✓	✓			
Deliberately accessing or trying to access offensive or pornographic material			✓	✓		✓			
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			✓	✓		✓			

16.2. Staff incidents

Staff incidents	Refer to line manager	Refer to Head	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓				
Inappropriate personal use of the internet / social media / personal email		✓						
Unauthorised downloading or uploading of files		✓						
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school/Trust network, using another person's account		✓						
Careless use of personal data e.g. holding or transferring data in an insecure manner		✓						
Deliberate actions to breach data protection or network security rules		✓		✓				
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓		✓				
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		✓						
Using personal email, social networking, instant messaging and/or text messaging to carry out digital communications with pupils		✓	✓					
Actions which could compromise the staff member's professional standing		✓						
Actions which could bring the school/Trust into disrepute or breach the integrity of the ethos of the school/Trust		✓						

Staff incidents	Refer to line manager	Refer to Head	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Using proxy sites or other means to subvert the academy's filtering system		✓			✓			
Accidentally accessing offensive or pornographic material and failing to report the incident		✓			✓			
Deliberately accessing or trying to access offensive or pornographic material		✓			✓			
Breaching copyright or licensing regulations		✓	✓					
Continued infringements of the above, following previous warnings or sanctions		✓	✓					

17. Links with other policies

This policy is linked to our:

- Child protection and safeguarding policy.
- School behaviour policies.
- Staff disciplinary procedures.
- Data protection policy and privacy notices.
- Complaints procedure.

Appendix 1: Acceptable use agreement – Staff, Members, Trustees, LAB/Committee members, volunteers, and visitors

I agree to follow the rules set out in the Trust's IT & Online Safety Policy.

When using the Trust's ICT systems and accessing the internet in school, or outside school on a Trust device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature.
- Use them in any way which could harm the Trust/school's reputation.
- Access social networking sites or chat rooms.
- Use any improper language when communicating online, including in emails or other messaging services.
- Install any unauthorised software.

Share my password with others or log in to the school's network using someone else's details.

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.

Name

Signature

Date

Appendix 2: Acceptable use agreement – pupils and parents/carers

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

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit.

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

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

Parent/Carer agreement

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

Name of pupil

Signature of pupil

Signature of parent/carer

Date
