Top Valley Academy

[E-Safety] Digital Technologies Policy

E Safety Policy

Approved by Governing Body 18 January 2016

Rationale

The policy aims to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely and are protected from potential harm, both within and outside the Academy. The policy also forms part of the Academy's protection from legal challenge, relating to the use of digital technologies.

New technologies have become integral to the lives of children and young people in today's society. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. Top Valley Academy believes that all users should have an entitlement to safe internet access at all times.

Top Valley Academy will continue to use the SWGFL 360 degree safe as an online tool to review their e-safety policy and practice. This tool provides an "improvement action" describing how the Academy might review and seek to improve its practice and allows comparison of levels to the benchmark levels of all schools using the tool. Further, Top Valley Academy intends to apply for assessment for the E-Safety Mark.

This policy was written in consultation with:

- Governors
- Teaching Staff and Support Staff
- Students
- Parents

Due to the ever changing nature of digital technologies the Academy will review the E-Safety Policy annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

The Academy will monitor the impact of the policy using:

- Logs of reported incidents
- Logs of internet activity (including sites visited)
- Internal monitoring data of network activity
- Surveys / questionnaires of
    - ✓ students
    - ✓ parents / carers
    - ✓ staff

Scope of the Policy

This policy applies to all members of Top Valley Academy community (including staff, students, volunteers, parents / carers and visitors), who have access to and are users of Academy ICT systems, both inside and outside of the Academy.

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of students 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 e-safety incidents covered by this policy, which may take place outside of the Academy, but is linked to membership of the Academy. The Academy will deal with such incidents within its Behaviour and Anti-Bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place outside of the Academy.

Where appropriate the Academy, in line with its published Behaviour policy, may choose to use the powers provided to it under the 2011 Education Act with regard to the searching for and inspection of electronic devices and any subsequent deletion of data.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the Academy.

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body is a member of the E-Safety Group.

Headteacher and Senior Leaders:

The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the Academy and its community, although the day-to-day responsibility for e-safety will be delegated to a nominated person.

The Headteacher and Senior Leadership Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Senior Leaders are responsible for ensuring that all relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

A member of Senior Leadership will be a member of the E-Safety group.

E-Safety Group:

This group is made up of the following:

- Member of the Senior Leadership Team (E-Safety Lead)
- Behaviour Lead
- Safeguarding Lead Professional
- Network Manager
- Governor
- Social Media Administrator

The E-Safety Group provides a working group that has wide representation from the Academy community, with responsibility for issues regarding e-safety and the monitoring/reviewing of the e-safety policy including the impact of initiatives. The group will also be responsible for:

- The day to day responsibility for e-safety issues and establishing and reviewing the Academy's e-safety policies / documents
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Providing training and advice for staff
- Receiving and reviewing reports of e-safety incidents and creating a log of incidents to inform future e-safety developments.
- Meeting regularly to discuss current issues, review incident logs and filtering / change control logs
- Attending relevant meeting of Governors
- Reporting regularly to Senior Leadership Team
- Ensuring that the Academy's technical infrastructure is secure and is not open to misuse or malicious attack
- Ensuring that the Academy meets the required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- That filtering is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- Keeping up to date with e-safety technical information in order to effectively carry out e-safety roles and to inform and update others as relevant
- Ensuring that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the members of the E-Safety group for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in the Academy's policies

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the Academy e-safety policy and practices.
- They have read, understood and accepted the terms of the Staff Acceptable Use Policy
- They report any suspected misuse or problem for investigation / action / sanction – using the SIMS system
- All digital communications with students / parents / carers should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- Students understand and follow the e-safety and acceptable use policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other Academy activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

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

- A planned programme of formal e-safety training will be made available to staff.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the Academy's e-safety policy and Acceptable Use Agreements.
- The E Safety group will receive regular updates through attendance at external training events
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- Governors to participate in e-safety training / awareness sessions, with particular importance for those who are members e-safety / health and safety / child protection groups.

Students:

- Are responsible for using the Academy digital technology systems in accordance with their Student Acceptable Use Policy.
- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the Academy's E-Safety Policy covers their actions out of school, if related to their membership of the Academy

The Academy believes that the education of students in e-safety is an essential part of the Academy's e-safety provision. Children and young people need to be taught to recognise and avoid e-safety risks and build their resilience. E-safety should be a focus across all areas of the curriculum and staff should reinforce e-safety messages. E-safety will be provided in the following ways:

- A planned e-safety curriculum will be provided as part of Computing / PHSE / ICT lessons
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students will be helped to understand the need for the Student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside the Academy.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Parents / Carers/Community

- Parents / Carers are responsible for using the Academy digital technology in accordance with the Acceptable Use Policy.
- Play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way.

- Will be encouraged to support the Academy in promoting good e-safety practice and to follow guidelines on the appropriate use of digital technologies.

The Academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. 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 Academy will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, VLE
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to relevant web sites / publications
- Providing family learning courses in use of new digital technologies, digital literacy and e-safety
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The Academy website will provide e-safety information for access by the wider community.

Technical (infrastructure / equipment, filtering and monitoring)

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

In fulfilling its safeguarding duty under the Counter-Terrorism & Security Act 2015, Top Valley Academy will use filtering and monitoring software to ensure students are safe online from terrorist and extremist material when accessing the internet in school.

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing in their own technologies in order to provide a greater freedom of choice and usability. If and when the Academy decide to implement BYOD a policy will be implemented.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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 students 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.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at Academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow Academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Academy equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the Academy into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with ~~good practice~~ the Academy's guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Permission from parents or carers ~~will be~~ is obtained before photographs of students are published on the school website – The Academy's use of images information (see below) is distributed annually and parents/cares are required to inform the Academy if they do not agree to the use of images of their child.

Images - Conditions of Use

1. We will not use the personal details or names (which means first name **and** surname) of any student in a photograph on our website, in our Academy prospectus or in any of our other printed publications without the express permission of parent(s)/carer(s) to do so.

2. We will not include personal e-mail or postal addresses, or telephone or fax numbers on our website, in our Academy prospectus or in other printed publications.

3. If we use photographs of individual students, we will not use the full name of that student in the accompanying text or photo caption without the express permission of parent(s)/carer(s) to do so.

4. If we name a student in the text, we will not use a photograph of that student to accompany the article.

5. We may include pictures of students and teachers that have been drawn by the students.

6. We may use group or class photographs or footage with very general labels, such as "a science lesson" or "making Christmas decorations".

7. We will only use images of students who are suitably dressed, to reduce the risk of such images being used inappropriately.

8. If images are taken by local press/media, or parents/guests, the Academy will not have control of these images but will ensure that we do not issue the first name and surname of students without the express permission of parent(s)/carer(s) to do so.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. (See Data Protection Policy and Code of Conduct)

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.
- Only transfer data using encryption and secure password protected devices.

Staff are advised, due to the sensitive nature of student data, not to transfer such information to portable devices instead using the access provided by (VLE) The Hub system available.

If personal data has to be stored on any portable computer system, memory stick or any other removable media then:

- The Network Manager must be consulted to ensure adequate encryption is in place.
- The data must be encrypted and password protected
- The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, once it has been transferred or its use is complete.

Social Media - Protecting Professional Identity

(In conjunction with Top Valley Academy's Staff Social Networking Policy and Code of Conduct)

Academy staff should ensure that:

- No reference should be made in social media to students, parents / carers or Academy staff
- They do not engage in online discussion on personal matters relating to members of the Academy community
- Personal opinions should not be attributed to the Academy
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The Academy's own use of social media for professional purposes will be reviewed regularly by the E-Safety group.

Responding to Safeguarding Concerns - Incidents of Misuse /Unsuitable / Inappropriate activities

This procedure does not include incidents classified as misuse of ICT where pupils are off task in a classroom environment accessing sites such as gaming or Google maps. These should be dealt with through the SIMS 'C' behaviour system in line with the behaviour policy.

Illegal Incidents

If there is any suspicion that the incident may involve child abuse images, or if there is any other suspected illegal activity (e.g. adult material which potentially breaches the Obscene Publications Act, racist material etc.) report immediately to the Headteacher/Lead Professional for Safeguarding/Police and act to preserve evidence

Other Incidents

It is hoped that all members of the Academy community will be responsible users of digital technologies, who understand and follow the Academy policies. 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 / volunteer 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.
- 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 incident investigation log (appendix 1), 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 Local Authority or national / local organisation (as relevant).
    - 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
    - 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 Academy and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.

Agreed action to be taken in the event of:

1. Inappropriate but not illegal use (bullying, adult content i.e. jokes, violent action films).

   Or

2. Illegal material or activity (grooming, sexually explicit material shared with child, child abuse images)

An <u>inappropriate</u> website is accessed <u>unintentionally</u> in the Academy by a teacher/member of staff or child.

- Play the situation down; don't make it into a drama.
- Report via email for a concern regarding a teachers/member of staff
- Complete the E-Safety Safeguarding incident log on SIMS for child

Following investigation in conjunction with the Lead Professional for Safeguarding or E-Safety Lead:

- A decision will be made whether to inform the parents of any student who viewed the site
- Ensure the Network Manager is aware to enable the site to be filtered

An <u>inappropriate</u> website is accessed <u>intentionally</u> by a child.

- Complete the E-Safety Safeguarding incident log on SIMS

Following investigation in conjunction with the Lead Professional for Safeguarding or E-Safety Lead:

- A decision will be taken about notifying the parents of the site accessed.
- Refer to the Acceptable Use Policy that was accepted by the student, and apply agreed sanctions in line with behaviour policy.
- Ensure the site is filtered (if need be) and notify the Network Manager.
- Notify TVA Lead Professional for Safeguarding.

An adult uses School IT equipment <u>inappropriately.</u>

- Report the misuse **immediately** to the Headteacher/SLT/Lead Professional for Safeguarding who will ensure that there is no further access to the PC or laptop.

Following investigation in conjunction with the Lead Professional for Safeguarding:

If the material is offensive but **not illegal**:

- Remove the PC to a secure place.
- Ensure you have a colleague with you, do not view the misuse alone.
- Instigate an audit of all ICT equipment to ensure there is no risk of students accessing inappropriate materials in the school.
- Identify the precise details of the material.
- Take appropriate disciplinary action.
- Inform governors of the incident.

In an extreme case where the material is of an **illegal** nature:

- Contact the local police and follow their advice.
- If requested, to remove the PC to a secure place and document what you have done. This is most important, as successful prosecutions depend on a secure chain of evidence.

A <u>bullying incident</u> directed at a student occurs through email or mobile phone technology, either inside or outside of school time.

- Advise the student not to respond to <u>or</u> delete the offending item(s).
- Complete the E-Safety Safeguarding incident log on SIMS.

Following investigation in conjunction with the Lead Professional for Safeguarding:

- Inform the Lead Professional for Safeguarding & Headteacher
- Refer to relevant policies including e-safety/ anti-bullying/behaviour and apply appropriate sanctions (TVA Student Support).
- Secure and preserve any evidence.
- Inform the sender's e-mail service provider.
- Notify parents of the students involved (TVA Student Support).

Malicious or threatening comments are posted on an Internet site about a student or member of staff.

- Complete the E-Safety Safeguarding incident log on SIMS for a pupil
- Report via email if connected to a member of staff.

Following investigation in conjunction with the Lead Professional for Safeguarding:

- Inform and request the comments be removed if the site is administered externally.
- Inform Lead Professional for Safeguarding & Headteacher deal with internally in line with behaviour policy if appropriate.
- Secure and preserve any evidence.
- Send all the evidence to CEOP/police
- Endeavour to trace the origin and inform police if appropriate.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with a student

- Report it immediately to the Head teacher or the Lead Professional for Safeguarding who will:
    - Contact parents.
    - Inform Headteacher and E-safety group members.
    - Advise the student on how to terminate the communication and save all evidence.
    - Contact CEOP/police
    - Consider the involvement social services.

- Complete the E-Safety Safeguarding incident log on SIMS

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

Any other concerns that a child's safety is at risk or concerned about the actions of a member of staff in any other circumstance other than those mentioned above

- Report using the E-Safety Safeguarding incident log on SIMS for pupils
- Raise any concerns about a member of staff via email
- Discuss with the Lead Professional for Safeguarding who will decide if any action should be taken.

Academy Actions & Sanctions

It is more likely that the Academy 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. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures/ Behaviour policy.

Password Security

A safe and secure password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE/ The Hub).

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the E-Safety Committee.
- All Academy networks and systems will be protected by secure passwords that are changed on a regular basis/prompted for change by the computer systems automatically
- The “master / administrator” passwords for the Academy systems, must be known by 4 staff members who have committed to non-disclosure and non-use except in emergencies. IT technical staff use these passwords on a daily basis.
- A copy of the passwords will be stored in the safe to provide SLT access for general non-use except in emergencies.
- Passwords for new users, and replacement passwords for existing users will be allocated by IT technical staff as a default and changed at the first login by the member of staff.
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Users will change their passwords at regular intervals.
- The level of security required may vary for staff and student accounts and the sensitive nature of any data accessed through that account.

Staff passwords:

- All staff users will be provided with a username and password by the systems manager.
- The password should be a minimum of 8 characters long and must include one of each of the following, an uppercase character, a lowercase character, a number and a special character, e.g. 32%TrgQT
- Must not include proper names or any other personal information about the user that might be known by others
- The account should be “locked out” following six successive incorrect log-on attempts
- Temporary/new passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- Passwords should be different for different accounts (except for Single Sign On, SOS), to ensure that other systems are not put at risk if one is compromised and should be different for school systems to those use for personal systems
- Should be changed at least every term.
- Should not re-used for 6 months and be significantly different from previous the last four passwords cannot be re-used passwords created by the same user.
- Should be different for school systems to those of personal systems

Members of staff will be made aware of the Academy's password policy:

- At induction
- Through the Academy's E-safety policy
- Through the Acceptable Use policy

Student passwords

The Academy will allocate individual usernames and passwords to students.

- All users will be provided with a username and password.
- Users will be required to change their password every term.
- Students will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Students will be made aware of the Academy's password policy:

- In lessons
- Through the Acceptable Use policy

Appendices

1. Incident Log

Appendix 1

E-safety Safeguarding Incident Log

Details of incident

Time	Date
Where did the incident occur:	
Name and contact details of person reporting incident	
Who was involved in the incident	☐ child/young person ☐ staff member ☐ other (please Specify) _____
Names and details of those involved:	

Type of incident	☐ bullying or harassment ☐ accessing inappropriate website/content ☐ online bullying or harassment (cyberbullying) ☐ sexting (self-taken indecent imagery) ☐ deliberately bypassing security or access ☐ hacking or virus propagation ☐ racist, sexist, homophobic religious hate material ☐ terrorist material ☐ other (please specify)_____
Description of incident:	
Nature of incident	☐ deliberate access ☐ accidental access
Did the incident involve material being	☐ created ☐ viewed ☐ printed ☐ shown to other ☐ transmitted to others ☐ distributed ☐ other (please specify)_____
Could this incident be considered as	☐ harassment ☐ grooming ☐ cyberbullying ☐ sexting (self-taken indecent imagery) ☐ breach of AUP ☐ other (please specify)_____

Action taken	☐ **staff** ☐ incident reported to Head teacher/senior manager ☐ advice sought from children's social care ☐ incident reported to police ☐ incident reported to CEOP ☐ incident reported to Internet Watch Foundation ☐ incident reported to IT Network Manager ☐ disciplinary action to be taken ☐ e-safety policy to be reviewed/amended ☐ other (please specify)_____ ☐ **child/young person** ☐ incident reported to member of staff (specify) _____ ☐ incident reported to social networking site ☐ incident reported to IT ☐ child's parents informed ☐ disciplinary action taken ☐ child/young person debriefed ☐ e-safety policy to be reviewed/amended ☐ other (please specify)_____

Outcome of incident/ investigation (To be completed by E-Safety or Safeguarding Lead)

Individual (staff member/child)
Police/CEOP
Organisation
Children's social care
Other (HR/legal etc.)

Learning from the case

Key learning point 1
Key learning point 2
Key learning point 3

Key learning point 4

Recommendations and timescales to implement

Recommendation 1	Timescale to be implemented
Recommendation 2	Timescale to be implemented
Recommendation 3	Timescale to be implemented
Recommendation 4	Timescale to be implemented

Signed	Print name Date
Signed	Print name Date
Signed	Print name Date
Signed	Print name Date