Unit 19, Avenue B,
Nottingham,
NG1 1DU

FAST FORWARD
Acceptable Use of Technology & E-Safety Policy

Overview

FAST FORWARD is an DJ & Music Studies provision who caters for up to 70 students aged 11-18 years who attend on a different ratio of days a week. We cover NCC and Nottinghamshire schools/partnerships. The students exhibit a variety of complex educational, social, emotional and mental health difficulties, which have impeded personal developmental and educational success.
Some of the students have stated diagnoses. Some of our learners have visited a variety of Alternative Provisions or Schools prior to attending FAST FORWARD. They can arrive at FAST FORWARD very disengaged with education and home life.

Introduction

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, Education Providers need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Within this, Education Providers equally have a duty to ensure that this is done safely and to ensure that pupils are taught about the importance of staying safe online and the responsible use of technology.

AIMS of the Policy

- To establish the ground rules, we have at FAST FORWARD for using any technology
- To describe how these fit into the wider context of other policies that are relevant e.g., Safeguarding, Code of Conduct, Behaviour etc
- To demonstrate the methods used to protect children from sites containing any material that is deemed to be inappropriate or harmful because of content that is pornographic, sexually explicit, violent, extremist or radicalising, or discriminatory on the grounds of any of the 7 protected characteristics in the Equality Act 2010.

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

• Websites
• Apps
• E-mail - Instant Messaging and chat rooms
• Social Media, including Facebook and Twitter
• Mobile/ Smart phones with text, video and/ or web functionality
• Other mobile devices including tablets and gaming devices
• Online Games
• Learning Platforms and Virtual Learning Environments
• Blogs and Wikis
• Podcasting
• Video sharing
• Downloading
• On demand TV and video, movies and radio / Smart TVs

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

Technology Covered in this Policy

This policy (for all staff, regular visitors, parents [for regulated activities] and pupils) is inclusive of both fixed and mobile internet; technologies provided by FAST FORWARD (such as PCs, laptops, mobile devices, digital video equipment, etc); and technologies owned by pupils and staff.

Background
Definition of Safeguarding

Safeguarding children and protecting them from harm is everyone's responsibility. Everyone who comes into contact with children and families has a role to play. The following is the accepted definition of 'Safeguarding' and the promotion of wellbeing for children:

• protecting children from maltreatment;
• preventing impairment of children's health or development;
• ensuring that children grow up in circumstances consistent with the provision of safe and effective care;
• taking action so as to enable children to have optimum life chances and enter adulthood successfully and have the best outcomes;

Local authorities/Education Provisions have overarching responsibility for safeguarding and promoting the welfare of all children and young people in their

area. They have a number of statutory functions under the 1989 and 2004 Children Acts which make this clear, and this guidance sets these out in detail. Further changes were made by the Children and Social Work Act 2017**,** which amended the 2004 Act in a number of areas.

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

Further information on this can be found in Keeping Children Safe in Education Policy 2022. Safeguarding and Child Protection Policy. GDPR Policy Updated 2022.

Definition of E-Safety

In addition to the definition set out in above, the term e-safety is specifically defined for the purposes of this document as the process of limiting the risks to children and young people when using Internet, Digital and Mobile Technology (IDMTs).

FAST FORWARD's vision is that all students, parents/carers and all those working with children recognise these risks and potential dangers that may arise from the use of technology in all forms, that they understand how to mitigate these risks and are able to recognise, challenge and respond appropriately to any e-safety concerns so that students are kept safe.

Potential Risks

We have a greater understanding of the extent of day-to-day dangers the virtual world can pose to children, including:

- being groomed online by adults with the ultimate aim of exploiting them Sexually.
- being bullied by others via social networking sites etc known as cyber Bullying.
- the taking of inappropriate / indecent images of children which are then uploaded and circulated via websites or networking sites. This is a criminal offence under s45 of the Sexual Offences Act.
- the exposure of children to inappropriate / indecent / harmful images or material – including violence, sexual content (including pornography), content that is discriminatory on the grounds of race, gender, sex, religion, disability or sexual orientation.
- being exposed to the glorification and promotion of gang culture through gang websites, chat rooms, forums.
- the targeting of children by groups wishing to radicalise children online through content that appears on websites, chat forums or direct contact (e-mail / social media).

Ignoring these dangers would be a breach in our responsibilities in Working Together to Safeguard Children 2018 and updated in 2022.

FAST FORWARD
Direction Thru Music

Unit 19, Avenue B,
Nottingham,
NG1 1DU

E-Safety Complaints

Please follow the FAST FORWARD Allegations and Complaints Policy. Whistle Blowing Policy, Data Protection Policies.

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

All factors in relation to the complaint must be clearly established in order to have substance. Complaints about an employee's IDMT misuse should be escalated to the Safeguarding and Director's immediately and be managed according to our KCSiE 2022 Policy. We have the ability to scrutinise IDMT (Institute of Digital Media Technology**)** use in particular, we have the ability to identify sites accessed. Potentially illegal issues must always be referred to the police in the first instance.

SECTION ONE – Keeping Children and Young People Safe
Education and Learning

FAST FORWARD **do not** provide internet access to children directly and we ensure that this is done in a way that is safe and age appropriate, by way of appropriate filtering systems. Our children do access internet via own mobile devices using own data, **no** access to the Wi-Fi is given to pupils here at FAST FORWARD. Thus, to avoid any access to Social Media sites etc.

Throughout the curriculum and class/studio workshops, all students are taught about the risks and responsibilities as well as the educational rewards of using technology.

Students are taught to:

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

Filtering

Levels of internet access and supervision must be appropriate and suitable for the students - however we recognise that there may be websites that staff may wish to

access for research that might normally be filtered out e.g., google images. Access controls (filtering) fall into several categories:

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

Illegal Downloading

Students are made aware that if they attempt to download copyright protected files, they are breaking the law or infringing intellectual property rights. Our Administration ICT network does not permit any child to download anything. Students do not have access directly to the internet at FAST FORWARD.

Cyber-Bullying

Cyber bullying is defined as the act of using the Internet, mobile phones, video games, or other technology gadgets to send, text, or post images or other material intended to hurt or embarrass another person. “It is also defined as acts of aggression through computers, mobile phones, and other electronic devices” (Jackson & Cohen, 2012)

At FAST FORWARD we have a zero-tolerance policy on this kind of behaviour. The law gives schools/alternative provisions the power to intervene in such cases even when they have happened outside of education time, using technology that is not the provision.

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

The following are the most commonly reported types of cyberbullying:

• Email – Can be sent directly to an individual or group to encourage them to participate in the bullying and can include derogatory comments or harassment.
• Instant messaging – messages can be sent directly to an individual or group who can then be included in the conversation.
• Social networking sites – anonymous profiles can be set up to make fun of someone and each person contributing to these pages can soon worsen the problem.
• Inappropriate and threatening comments and images can also be posted and circulated without consent.
• Mobile Phones – Anonymous and abusive text or video messages and photo messages and phone calls can be shared via phones. This includes the videoing and sharing of physical or sexual attacks (a criminal offence) on individuals.
• Interactive gaming – Games consoles allow users to chat online with anyone.
• Abuse of other online game players and the use threats.
• Hacking into the account of another user for malicious reasons

• Sending viruses – These can be sent from one person to another in order to destroy computers or delete personal information from their hard drive.
• Abusing personal information – Personal / sensitive information (including videos and photographs) being uploaded onto the internet without the victim's permission.

Some instances of cyberbullying do escalate into physical bullying. We take all instances of cyberbullying extremely seriously and we record all instances that are reported to us. We will escalate concerns to the police where necessary. We encourage children to store the electronic records of abuse which will be essential in any subsequent investigation.

Monitoring E-Safety Incidences and Reporting Abuse

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

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

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

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

• A description of the e-safety incident
• Who was involved
• How the incident was identified
• What actions were taken and by whom
• Conclusion of the incident
• Lessons learnt – to inform ongoing policy and practice

Children Sending Emails

No student at FAST FORWARD is able to send emails within the provision.

Students and Mobile Phones

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

FAST FORWARD
Direction Thru Music

Unit 19, Avenue B,
Nottingham,
NG1 1DU

Students with Additional Needs

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

Involving Parents and Carers

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

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

SECTION TWO – Keeping Adults Safe

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

Monitoring

All monitoring, surveillance or investigative activities are conducted by FAST FORWARD designated ICT support staff and comply with the GDPR Act 2018 (updated 2022), the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Personal Data

FAST FORWARD
Direction Thru Music

Unit 19, Avenue B,
Nottingham,
NG1 1DU

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

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

New GDPR regulations of 2018 (updated 2022) have key areas of changes; the most significant changes that will take affect how we all work is in additional rights afforded to individuals. These allow individuals to request access, corrections and removal of their personal information in ways that weren't available before.

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

Six principles of processing personal data are depicted in the GDPR 2018 (updated 2022) Legislation – see FAST FORWARD GDPR Policy/FAST FORWARD Deletion Policy on how we meet these guidelines.

Breaches

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

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

For staff any policy breach is grounds for disciplinary action in accordance with the FAST FORWARD Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated. Dealt with Senior Staff. Incidents will be reported to the GDPR Officer. Policy breaches may also lead to criminal or civil proceedings. See GDPR Policy relating to security breaches.

Staff Sending Emails

The use of e-mail within FAST FORWARD is an essential means of communication for both staff and partnership schools. For this reason, it is important that all staff check their email regularly, to ensure email archives are to a minimum. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer

significant benefits and we recognise that pupils need to understand how to use e-mail in relation to their age and how to behave responsible online. All using Password Protected Security emails in relation to pupil's data. Abbreviations for some names will be used. An audit for GDPR ensures all contact information is relevant and current. See FAST FORWARD GDPR/Deletion Policy.

Managing Email

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

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

An audit for GDPR ensures all contact information is relevant and current which FAST FORWARD hold, reviewed and updated regularly. Archived information from emails is kept on a hard drive. See FAST FORWARD GDPR/Deletion Policy.

FAST FORWARD requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the provision or the LEA'.

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

- Organise e-mail into folders and regularly delete old / unwanted mail.
- e-mails containing personal, confidential, classified or financially sensitive
- data sent to external third parties or agencies should be marked as
- confidential (refer to the Section 'E-Mailing personal, sensitive confidential or
- classified information')
- Use only your own FAST FORWARD e-mail account (not that of other staff members)
- Do not send / forward attachments internally unnecessarily.
- Do not use FAST FORWARD'S e-mail for personal business
- Never open attachments from untrusted sources; consult your network manager first
- Be aware that FAST FORWARD based email and internet activity can be monitored and explored further if required

FAST FORWARD
Direction Thru Music

Unit 19, Avenue B,
Nottingham,
NG1 1DU

Emailing Personal, Sensitive or Confidential / Classified Information.

Where e-mail must be used to transmit/process such data:

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

Personal Mobile Devices (including phones)

Staff are permitted to bring in personal mobile phones and devices for their own use. Under no circumstances should a member of staff contact a student or parent/ carer using their personal device use it or to take video footage or still images of students or any other school activity. Under GDPR contacts for parents/students or should be done via the main office or on a designated work phone.

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

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

FAST FORWARD Provided Mobile Devices (including phones)

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

Students and Staff emergency contacts are kept within the main office and given to staff via phone to contact parents/carers/schools, these are then deleted from the phone to ensure GDPR data protection regulations are met. At the end of the day.

FAST FORWARD
Direction Thru Music

Unit 19, Avenue B,
Nottingham,
NG1 1DU

Use of social media – have our own website.

Facebook, Twitter, Instagram, Snap Chat and other forms of social media are increasingly becoming an important part of our daily lives. FAST FORWARD uses Instagram and Facebook but with parental consent if names and photos are put onto it. This is another way FAST FORWARD try to communicate with parents and carers. At present FAST FORWARD does not have an official website.

In relation to social media, the following applies:

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

Use of Land Line Telephones

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

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

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

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

Keeping Data and Equipment Protected

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.

• Never interfere with any anti-virus software installed on IT equipment.
• If your machine is not routinely connected to the FAST FORWARD network, you must make provision for regular virus updates through the IT Support team.
• If you suspect there may be a virus on any FAST FORWARD IT equipment, stop using the equipment and contact your IT support provider immediately.
The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

Data Security

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

All staff should:

• keep all FAST FORWARD related data secure. This includes all personal, sensitive, confidential or classified data.
• avoid leaving any portable or mobile IT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked and out of sight.
• be responsible to ensure the security of any personal, sensitive, confidential and classified information contained in documents copied, scanned or printed.
• notify the recipient before sensitive / confidential messages are sent.
• read relevant policies in line with this policy.

All staff agree to:

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

Unit 19, Avenue B,
Nottingham,
NG1 1DU

• Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling.

Passwords and Passwords Security

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

Relevant Responsible Person

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

• to lead on the information risk policy and risk assessment
• to advise staff on appropriate use of the provision's technology
• to act as an advocate for information risk management
• what information is held, and for what purposes
• what information needs to be protected, how information will be amended or added/deleted to over time
• who has access to the data and why
• how information is retained and disposed of

For information such as assessment records, medical information and special educational needs data, a responsible member Steve Lee/Chris Goss of staff should be able to identify across the provision.

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

Disposal of Redundant IT Equipment

All redundant IT equipment will be disposed of. All redundant IT equipment that may have held personal data will have the storage archived onto a hard drive or erased in line with the Deletion Policy. This is to ensure the data is irretrievably destroyed, or if

the storage media has failed it will be physically destroyed. We will securely dispose of removable media that may hold personal data. It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not enough to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a written guarantee that they will irretrievably destroy the data by multiple over writing the data.

Disposal of any IT equipment will conform to:

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

The Provision will maintain a comprehensive inventory of all its IT equipment including a record of disposal which will include: In line with any GDPR requirements.

• Date item disposed of
• Authorisation for disposal, including:
• verification of software licensing
• any personal data likely to be held on the storage media? *
• How it was disposed of e.g., waste, gift, sale
• Name of person & / or organisation who received the disposed item
• Any redundant IT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

ZOMBIE ACCOUNTS

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

SERVERS

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

Review Procedure

There will be on-going opportunities for staff to discuss with the Safety coordinator any ESafety issue that concerns them (Ash Day).

This policy will be reviewed every (12) months and consideration will be given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way, amendments to GDPR for example.

Further help and support

Office – www.ico.org.uk – Data Protection

Current Legislation

In line with material that might be criminal, cause harm to young people or be otherwise unlawful.

- The GDPR Act 2018 (Updated 2022)
- The Telecommunications (Lawful Business Practice) (Interception of
- Communications) Regulations 2000
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998
- Freedom of Information Act 2000 (Amendment) EU Exit Regulations 2018

Other Acts Relating to ESafety/data protection:

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

Written by: Adele Meek (QA Consultant)

Approved by Director Steve Lee

12th October 2022 / Updated 31st August 2024.
Review August 31st 2025

Unit 19, Avenue B,
Nottingham,
NG1 1DU

Policy reviewed in line with Government Changes and FAST FORWARD will be updated via QA reviews, internal inspections and advisories.

Appendix A

E-Safety Concern and Record of Action

This form is to be used to record any incidences of cyberbullying or inappropriate use of technology that comes to our attention both in and out of FAST FOWARD time.

Name of Victim

Tutor group Site Date

Type of technology that has been misused

Where is the technology located?

Incident description

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

FAST FORWARD
Direction Thru Music

Unit 19, Avenue B,
Nottingham,
NG1 1DU

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

What actions were taken and by whom?

Conclusion of the incident and lessons learnt – how was it dealt with and what will we do differently next time?

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

Report Completed by:

Sign:

Name:

Seen by Safeguarding Lead/DPO/SLT

FAST FORWARD
Direction Thru Music

Unit 19, Avenue B,
Nottingham,
NG1 1DU

Dear Parent/ Carer

IT including the internet, e-mail and mobile technologies has become an important part of learning in our provision. We expect all students to be safe and responsible when using any IT.

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

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

Parent/ carer signature

We have discussed this document with ……..... (child's name) and we agree to follow the ESafety rules and to support the safe use of IT at FAST FORWARD.

Parent/ Carer Signature ……

Class …… Date ……

FAST FORWARD
Direction Thru Music

Unit 19, Avenue B,
Nottingham,
NG1 1DU

Student Acceptable Use Agreement/ESafety Rules

As a pupil at FAST FORWARD, I agree that:

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

FAST FORWARD
Direction Thru Music

Unit 19, Avenue B,
Nottingham,
NG1 1DU

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

Signed……

Print Name……

Internet Safety and Acceptable Use Policy for Staff & Authorised visitors

In line with our policy on e-safety/data protection it is requested that all those using technology within FAST FORWARD, read and sign the agreement below:

Internet Use

• Children and non-staff adults are not to use the Internet without staff supervision.
• Any web pages to be used for teaching purposes should be screened by a member of staff before use with children.
• Fire walls, content screening software or service providers with filtering facilities are to be used wherever possible.
• Children and non-staff adults are instructed in the responsible use of the Internet and are asked to report any unsuitable material directly to the DPO ESafety Co-ordinator a member of the Senior Leadership Team promptly.
• Unsuitable content which is not blocked via the filtering system should be reported to the DPO.
• The internet should be used for curriculum, professional and administration purposes only.
• No information which could lead to the unauthorised identification or contact of an individual student or adult by a member of the public may be published on the Internet.
• Photographs of students may only be published on the FAST FORWARD Facebook site (with parental permission) but the children should never be named.
• Private contact details of staff or children (other than the FAST FORWARD contact details) must not be published on the Internet.
• The use of or viewing of online gambling sites are strictly forbidden.

E-mail Use

• Excessive unsolicited emails i.e. 'spam' to be reported to a technology team member. Under no circumstances should any accompanying attachments be opened.

FAST FORWARD
Direction Thru Music

Unit 19, Avenue B,
Nottingham,
NG1 1DU

• Any FAST FORWARD business should only be conducted via their email system provided.
• Use of personal email accounts to conduct FAST FORWARD business is not permitted and email accounts should not be used for personal uses.
• No Personal e-mail accounts may be accessed by staff.
• Personal use of e-mail addresses of children is not permitted.
• Personal use of e-mail by visitors and those outside of those outside is not permitted, unless authorised by a staff member.
• No information which could lead to the unauthorised identification or contact of an individual child or adult by a member of the public may be emailed.
• No Photographs of children may be emailed via FAST FORWARD e-mail within the organisation freely.
• Staff and guests should be instructed in the responsible use of the ICT facilities.
• Staff and guests must not interfere with the work of others on the system either directly or indirectly.
• Staff must be aware that FAST FORWARD based email and internet activity is monitored and explored further if required
• The facilities must be used in a responsible manner, in particular, staff and guests must not deliberately view, create or transmit material that is deemed / likely to be deemed as:
• Obscene, defamatory or indecent
• cause annoyance, inconvenience, anxiety or offence.
• infringes the copyright of another person.
• Introducing or causing viruses on FAST FORWARD computer systems or networks.

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

FAST FORWARD
Direction Thru Music

Unit 19, Avenue B,
Nottingham,
NG1 1DU

Use and storage of Digital Images and Media

• Photographs and video taken of children should always be done using FAST FORWARD equipment, never using personal cameras or mobile phones owned by members of staff or any other individuals in FAST FORWARD.
• When pictures are stored on the network, they should be deleted once used and should never be stored beyond their purpose. Exceptions to this would be for school purposes such as the Newsletter, or photographs used for publication purposes/future units of study.
• Images of children at CAST should never be stored on home computers.
• CAST cameras which hold images of children should not be taken outside of the school unless on school business.

I agree to the terms set out in this agreement. I understand that Internet use and e-mail use may be monitored.

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

Signed……

Print Name……..